NCIIPC – QCI Initiative

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

Issue No. 1 | Feb 2024

**Scheme for**
**Cyber Security Management System**

**Additional Technical Criteria (Level 3)**

# 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 CAF has a 3-level architecture specifying requirements layer by layer in the form of technical criteria. The Basic Technical Criteria (BTC) (Level 1) specifies requirements which are applicable to all sectors. Built over it, is sector specific requirements (in this case power sector) termed as Supplementary Technical Criteria (STC) (Level 2).

This document specifies Additional Technical Criteria (ATC) (Level 3), herein after referred to as ATC (Level 3), for 'system security' requirements implemented in industrial control systems specific to power sector.

# ACKNOWLEDGEMENT

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

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) 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 the technical inputs of Shri U.K. Nandwani, former DG, STQC and Shri Mukesh Kumar, Sr. Manager, CEA.

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

Dr. Manish Pande
Director and Head
PADD, QCI

## Contributors

### 1. Steering Committee

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

## 2. Technical Committee

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

## 3. Certification Committee

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

**SECTION 1**

# INTRODUCTION

## 1. Background

1.1 The cyber security of critical infrastructure requires to implement various controls which are organisations, personnel, process and technology specifics. Further, these need to be contextualised for a specific sector such as power sector where some of the controls will get enhanced along with certain additional sector specific controls with distinctive characteristics, risks, and priorities. It is also desirable to consider the environment and technologies that drives this sector such as ICS for a robust security assurance.

1.2 In view of the above, the conformity assessment framework should be architected in a way to cover IT/ICS related generic requirements over layered with sectorial requirements coupled with overall system security requirements. Following are the envisaged levels of Technical Criteria/ Standards in a hierarchal approach:

1.2.1. Basic Technical Criteria (Level 1) hereinafter referred to as BTC (Level 1) - Horizontal criteria covering common cyber security requirements for all or a wide spectrum of critical information infrastructure, i.e. “Cyber Security Management System for IT/ICS system.

1.2.2. Supplementary Technical Criteria (Level 2) hereinafter referred to as STC (Level 2) - Semi horizontal criteria covering cyber security requirements for specific CII sectors, where such requirements are typical of the sector.

1.2.3. Additional Technical Criteria (Level 3) hereinafter referred to as ATC (Level 3) - Vertical criteria addressing cyber security controls for specific classes of systems in a CII sector. ATC (Level 3) criteria shall be considered appropriate and necessary for development where BTC (Level 1) and STC (Level 2) standards do not completely address the relevant cyber security requirements in order to ensure appropriate security resilience.

1.3 This document caters to CSMS for ATC (Level 3) prescribing additional controls pertaining to ‘system security’ related with ICS. This levels broadly covers system security requirements and security levels pertaining to Network and System Security of Industrial communication networks.

1.4 The landscape of the control system has evolved with the introduction of widely available, cost-effective Ethernet and Internet Protocol (IP) devices, along with Commercial Off-The-Shelf (COTS) devices. This evolution heightens the susceptibility of the control system to cybersecurity vulnerabilities and incidents. While a cybersecurity management system designed for typical IT systems can address some cybersecurity concern in control system environments, the unique characteristics of control system environments necessitate a tailored approach to cybersecurity management.

1.5 Special considerations must be given to the following points when formulating a cybersecurity management system for the control system:

1.5.1 **Availability & Reliability Requirements:** The control system is time-critical and operates continuously. Unexpected outages in systems controlling industrial processes are deemed unacceptable.

1.5.2 **Risk Management Requirements:** The control system operation underscores the crucial link between safety and security. Any security measure that compromises safety is unacceptable. Failure to manage control system security may result in potential

threats to human safety, loss of equipment, loss of intellectual property, or environmental harm.

1.5.3 **Cyber-Physical System:** The control system interacts with physical processes, leading to consequences in the control system environment that can manifest in physical events.

1.5.4 **Legacy & Resource Constraints:** Control systems typically employ intelligent electronic devices with real-time operating systems, often facing resource constraints. The extensive presence of legacy systems may lack desired features such as encryption capabilities, error logging, and robust password protection.

1.5.5 **Proprietary Communications Protocols:** Communication protocols and media used in control system environments for field device control and intra-processor communication are typically proprietary.

1.5.6 **Change Management:** The change management process, when applied to the control system, requires careful assessment by domain experts. Software updates in the control system environment are not straightforward due to dependencies and implications on production. Thorough testing by both the control application vendor and end user is necessary before implementation.

1.5.7 **Vendor Dependency:** The control system may lack a diversified and interoperable system, mostly depending on support solutions from the supplier. Third-party security solutions may be restricted due to ICS vendor license and service agreements, risking loss of service support if installed without vendor acknowledgment or approval.

1.5.8 **Component Lifetime:** In the control system environment, where technology is developed for specific use, the lifetime of deployed technology is often in the order of 10 to 15 years, sometimes longer.

## 2. Objective

This document provides an extension to the certification bodies already accredited to Cyber Security Management System (CSMS) Scheme BTC (Level 1) and STC (Level 2) certification and now interested to operate an accredited ATC (Level 3) certification specific to the power sector.

2.1. The principal objective of this document is to provide a uniform approach to the certification of CSMS for ATC (Level 3) by CBs as the basis for a multilateral recognition framework.

2.2. The process used in developing this certification scheme was to establish firstly the key cyber security additional controls for power sector and processes for CSMS of CSEs for ATC (Level 3) certification and then determine the methods by which these compliances can be demonstrated and evaluated.

## 3. Scope

The scope of this document covers CSMS life cycle processes which include defining certification criteria, application, audit planning, conduct of audit, certification, surveillance, re-certification, provisional approval system and rules for use of Scheme mark.

**Note:** The technical requirements covered in this document are in addition to BTC (Level 1) and STC (Level 2). The ATC (Level 3) shall be implemented after effective implementation of BTC (Level 1) and STC (Level 2).

## 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 (for ATC (Level 3))
Section 4: Certification Process
Section 5: Requirements for Certification Bodies
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 IS/ISO/IEC 27000 and its family of standards.
BTC (Level 1) and STC (Level 2) define various terms and definitions in para 5, Section 1:Introduction. The same may be referred for this document, wherever applicable. Additional terminologies used are defined below:

5.1. **Countermeasure:** Action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.
5.2. **Degraded Mode** - Mode of operation in the presence of faults which have been anticipated in the design of the control system.
5.3. **Demilitarized Zone** - Common, limited network of servers joining two or more zones for the purpose of controlling data flow between zones.
5.4. **Essential Function -** Function or capability that is required to maintain health, safety, the environment, and availability for the equipment under control.
5.5. **Least Privilege -** Basic principle that holds that users (humans, software processes or devices) should be assigned the fewest privileges consistent with their assigned duties and functions.
5.6. **Responsible Entities -** Responsible entities, as per the guidelines are those entities that serve various roles in the power sector and are sector participants with significant exposure to cyber threats. These entities include power generation companies, transmission companies, distribution companies, OEMs and system operators.
*(Source - India's Central Electricity Authority (CEA) issued the Cyber Security in Power Sector Guidelines 2021. The comprehensive guidelines are intended to help all power sector entities in India take measured steps to improve their overall cybersecurity posture and protect critical infrastructure from cyber-attacks through specific interventions)*
5.7. **Security Level -** Measure of confidence that the control system is free from vulnerabilities and functions in the intended manner.
5.8. **Service Provider -** Organisation (internal or external organisation, manufacturer, etc.) that has agreed to undertake responsibility for providing a given support service and obtaining, when specified, supplies in accordance with an agreement.

## 6. Abbreviations

| | |
|---|---|
| **AB** | **Accreditation Body** |
| **AMI** | Advanced Metering Infrastructure |
| **AT** | Assessment Team |
| **ATC** | Additional Technical Criteria |
| **BIS** | Bureau of Indian Standards |
| **BTC** | Basic Technical Criteria |
| **CA** | Certification Authority |
| **CAB** | Conformity Assessment Body |
| **CAF** | Conformity Assessment Framework |
| **CB** | Certification Body |
| **CC** | Certification Committee |
| **CEA** | Central Electricity Authority |
| **CII** | Critical Information Infrastructure |
| **CIP** | Critical Infrastructure Protection |
| **CO** | Consultancy Organisation |
| **CRM** | Cross Reference Matrix |
| **CRS** | Cybersecurity Requirements Specification |
| **CSE** | Critical Sector Entity |
| **CSMS** | Cyber Security Management System for IT/ ICS |
| **DMZ** | Demilitarized Zone |
| **DNS** | Domain Name Service |
| **DoS** | Denial of Service |
| **EMI** | Electromagnetic Interference |
| **EMS** | Environmental Management System |
| **FAT** | Factory Acceptance Testing |
| **FR** | Foundational Requirement |
| **FS** | Functional Safety |
| **FTP** | File Transfer Protocol |
| **GLONASS** | Global Navigation Satellite System |

| | |
|---|---|
| **GPS** | Global Positioning System |
| **HMI** | Human-Machine Interface |
| **HSE** | Health, Safety and Environmental |
| **HTTP** | Hypertext Transfer Protocol |
| **IDS** | Intrusion Detection System |
| **IACS** | Industrial Automation and Control System |
| **IAF** | International Accreditation Forum |
| **ICS** | Industrial Control System |
| **ICT** | Information and Communications Technology |
| **IEC** | International Electrotechnical Commission |
| **IP** | Internet Protocol |
| **IPS** | Intrusion Prevention System |
| **IS** | Indian Standards |
| **ISA** | International Society of Automation |
| **ISMS** | Information Security Management System |
| **ISO** | International Organisation for Standardisation |
| **IT** | Information Technology |
| **MSC** | Multi-stakeholder committee |
| **NABCB** | National Accreditation Board for Certification Bodies |
| **NC** | Non-conformity |
| **NCIIPC** | National Critical Information Infrastructure Protection Centre |
| **NIST** | National Institute of Standards and Technology |
| **NSAB** | National Security Advisory Board |
| **NSCS** | National Security Council Secretariat |
| **OEMs** | Original Equipment Manufacturers |
| **QCI** | Quality Council of India |
| **RA** | Resource Available |
| **RDF** | Restricted Data Flow |
| **RE** | Requirement Enhancement |
| **RJ** | Registered Jack |
| **RTU** | Remote Terminal Unit |

| | |
|---|---|
| **SAT** | Site Acceptance Testing |
| **SC** | Steering Committee |
| **SCADA** | Supervisory Control and Data Acquisition |
| **SHA** | Secure Hash Algorithm |
| **SI** | System Integrity |
| **SIEM** | Security Information and Event Management |
| **SIF** | Safety Instrumented Function |
| **SIL** | Safety Integrity Level |
| **SIS** | Safety Instrumented System |
| **SL** | Security Level |
| **SL-A** | Achieved Security Level. |
| **SL-C** | Capability Security Level |
| **SL-T** | Target Security Level |
| **SM** | Skill Module |
| **SOA** | Statement of Applicability |
| **SR** | System Requirements |
| **SSH** | Secure Socket Shell |
| **STC** | Supplementary Technical Criteria |
| **SuC** | System under Consideration |
| **TC** | Technical Committee |
| **TCP** | Transmission Control Protocol |
| **TPM** | Trusted Platform Module |
| **TRE** | Timely Response to Events |
| **UC** | Use Control |
| **USB** | Universal Serial Bus |
| **VoIP** | Voice over Internet Protocol |
| **ZCR** | Zone and Conduit Requirements |

**SECTION 2**

# GOVERNING STRUCTURE

## 1. Objective

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

## 2. Scheme Owner and Scheme Manager

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

### 2.1 Roles and Responsibilities of the Scheme Owner

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

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

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

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

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

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

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

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, ensure that the information is also made available to all the bodies within the Scheme.

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

2.2.7 As the provider of provisional approval, mandate the approved CBs to provide reasonable access and cooperation as necessary to enable the QCI assessment team, which includes assessors, technical experts, observers, and regulators to assess conformity with the Agreement and as per the 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 CBs are processed expeditiously. Investigation and decision on complaints shall not result in any discriminatory actions.
The detailing of the activities of the Scheme Manager shall be such that it would independently operationalise the Scheme taking due care of issues such as impartiality, free from any conflict of interest etc.
Note 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 CBs' clients, wherever necessary, and other parties interested in the Scheme.

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

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

## 3. Governing Structure

3.1 The governing structure of the Scheme consists of a multi-stakeholder Steering Committee (SC) at the apex level, supported by a Technical Committee (TC), and a

Certification Committee (CC). The Secretariat will be provided by QCI (being the National Accreditation Body and Scheme Manager) on behalf of NCIIPC (being the Scheme Owner).

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

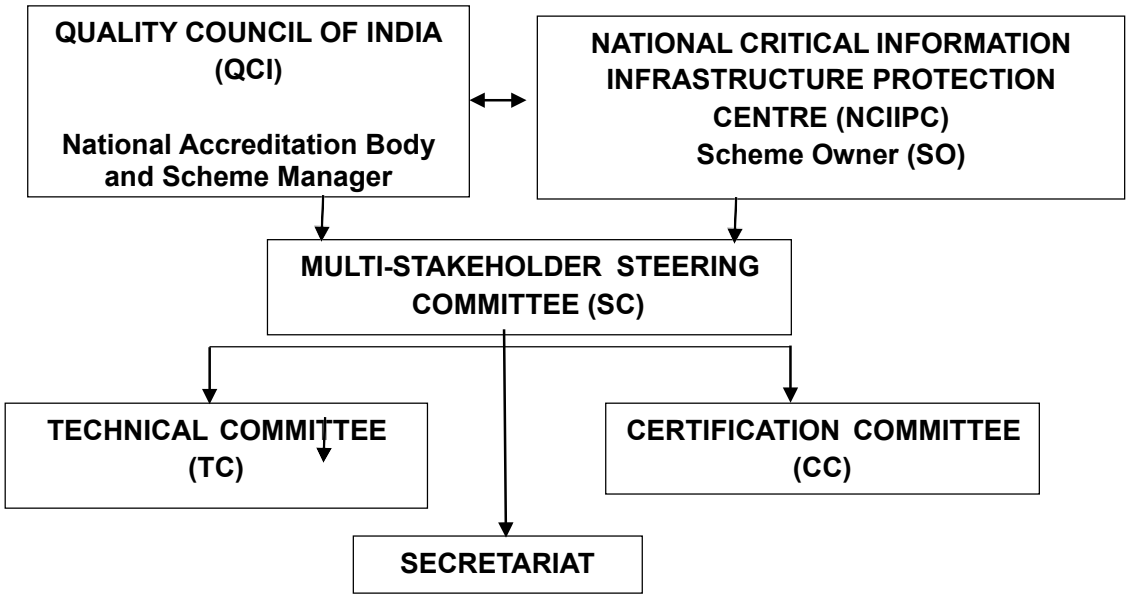


*Figure 2.1: Governing Structure*

3.3 **Appointment of Committees – General Rules**
In the appointment of various committees, the following general principles shall be kept in mind:

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

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

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

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

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

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

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

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

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

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

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

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

## 4. Multi-stakeholder Steering Committee (SC)

### 4.1 Membership

The SC shall comprise of the following:

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

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

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

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

4.1.5 Secretariat – Quality Council of India

### 4.2 Terms of Reference

The SC is responsible for the following:

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

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

4.2.3 Constituting any committees as needed.

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

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

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

4.3 **Meetings**

The SC shall meet at least once every year.

**5. Technical Committee (TC)**

5.1 **Membership**

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

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

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

5.1.3 National nodal agencies for Cyber security

5.1.4 Critical sector entities.

5.1.5 Industry Associations focused on critical sectors.

5.1.6 Knowledge Bodies/ Labs/ Consultation Organisations working in Cyber security.

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

5.1.8 Secretariat – Quality Council of India

5.2 **Terms of Reference**

The Technical Committee is responsible for the following:

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

5.2.2 Providing overall direction and guidance on the current cyber security issues and concerns necessary to be addressed.

5.2.3 Providing direction and guidance on the appropriate technical connotation of the audit.

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

5.2.5 Defining and formulating the technical content of the examination/ assessment process employed by the Scheme, and any of the accredited CBs.

5.2.6 Deliberations on any other applicable technical requirements.

5.3 **Meetings**

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

## 6. Certification Committee (CC)

### 6.1 Membership

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

6.1.2 Government Organisations.

6.1.3 Critical Sector Entities.

6.1.4 Industry associations.

6.1.5 Academic Institutions/ Training Bodies.

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

6.1.7 Secretariat – Quality Council of India.

### 6.2 Terms of Reference

The Certification Committee is responsible for the following:

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

6.2.2 Developing, maintaining, and revising as appropriate the documents such as certification process and requirements for CBs for CBs to apply for accreditation.

6.2.3 Developing, maintaining, and revising as appropriate the document i.e. provisional approval system for CBs to apply for accreditation.

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

6.2.5 Deliberations on any other issue relating to Certification of CBs.

### 6.3 Meetings

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

## 7. Roles of Organizations

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

7.2 Quality Council of India is the National Accreditation Body and Scheme Manager who will manage and operationalise the Scheme as per the established norms on behalf of Scheme Owner. It shall establish the MSC in consultation with Scheme Owner and shall be responsible for the overall management of the Scheme. QCI shall provide the Secretariat to the Scheme.

7.3 The National Accreditation Board for Certification Bodies (NABCB), a constituent Board of the QCI, shall be responsible for accrediting CBs desirous of participation in the Scheme. NABCB shall, through a legally enforceable agreement with the accredited CB, ensure that the CB 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 CB shall also provide access to NABCB assessors, experts and observers, to its premises to conduct assessment activities. The access to NCIIPC personnel or any personnel nominated by them will be similar to that of NABCB.

## 8. Complaints

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

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

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

8.4 Any complaint received by QCI shall be similarly handled.

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

## 9. Appeals

9.1 An appeal is a request by a CB to the AB for reconsideration of a decision made by that body.

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

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

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

9.5 In handling appeals, the broad principle that the appeal is handled independently, of the personnel involved in the decision, shall be maintained.

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

## 10. Review of the Scheme

The Scheme shall be reviewed for its relevance to the existing milieu at least once every year for 3 years from the launch and subsequently once in 5 years or earlier, as per requirement. The consideration while reviewing shall also include the review of past performance data related to approved CBs, the status of complaints/ appeals/ RTIs/ and any relevant information.

**SECTION 3**

# CERTIFICATION CRITERIA ADDITIONAL TECHNICAL CRITERIA (LEVEL 3)

## 1. Objective

1.1 A three-level architecture with technical requirements has been envisioned for the cybersecurity of Critical Information Infrastructure (CII). BTC (Level 1) is primarily based on the Information Security Management System (ISMS) standard (IS/ISO/IEC 27001:2022) with additional controls. This level is foundational in nature and common across all Critical Sector Entities (CSEs). STC(Level 2) enhances BTC (Level 1) by incorporating additional sector-specific Cyber Security Management System (CSMS) requirements outlined in IS/ISO/IEC 27019:2017. Applicable requirements from the IEC 62443 series of standards are also integrated in STC (Level 2).

**Note:** Basic Technical Criteria (Level 1), Supplementary Technical Criteria (Level 2) and Additional Technical Criteria (Level 3) are also referred to as BTC (Level 1), STC (Level 2) and ATC (Level 3) respectively.

1.2 ATC (Level 3) in addition to BTC (Level 1) and STC (Level 2), has been formulated to define control system requirements. These requirements are derived from a combination of functional requirements and risk assessments and aligned with the IEC 62443 series of standards, and Guide to Operational Technology (OT) Security, NIST Special Publication (NIST SP) 800-82r3 which specifically address the security of control systems.

1.3 This document outlines cybersecurity requirements for the Control System and determines the cybersecurity controls necessary for their safe and secure operations. The utility is obligated to comply with the requirements specified in the document to enhance the cybersecurity of the Control System.

1.4 The objective of Level 3 document is:

1.4.1 To define Technical Criteria addressing common set of security requirements of 'Control System'.

1.4.2 Enable all the utilities in power sector to define and implement mechanism to meet this technical criteria by providing the rationale and wherever applicable, implementation guidelines for the requirements.

1.4.3 Enable certification bodies to prepare audit criteria and checklist based on this technical criteria and conduct CSMS audit of CSEs.

1.4.4 Enable training bodies to design training material around the criteria.

1.4.5 Enable consultancy organisations to structure their consultancy profiles around the criteria.

## 2. Scope

2.1 The scope of ATC (Level 3) covers system security requirements and security levels of industrial control systems. These requirements are covered in the form of technical criteria. The scope of ATC (Level 3) is in progression to BTC (Level 1) and STC (Level 2) rather than being mutually exclusive and specific to the context of ICS.

2.2 Once Technical Requirements – BTC (Level 1) and STC (Level 2) have been implemented, CSEs are required to implement controls mandated in ATC (Level 3).

## 3. Intended Stakeholders

3.1 Any utility in the power sector seeking certificate from CBs for the compliance of their CSMS to ATC (Level 3).

3.2 Certification Bodies (CBs) and Inspection Bodies (IBs).

3.3 Accreditation Body.

3.4 Regulatory and National nodal agencies: NCIIPC, CERT-In, CEA etc.

3.5 Authorised Training bodies and Consulting Organisations, national bodies that are responsible for cybersecurity of Power Sector.

3.6 Implementers and Auditors of CSMS ATC (Level 3).

3.7 OEMs, Suppliers, Vendors, Software Developers and System Integrators of IT, SCADA, Control System and other components being used in the power supply system.

3.8 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. E.g., central and distributed process control, monitoring, and automation technology as well as vendors/OEM/system integrator of cyber systems used for their operation, such as:

- Programming and parameterization devices.
- Digital controllers and automation components
- Digital sensor and actuator elements,
- Control and field devices or Programmable Logic Controllers (PLCs) including Advanced Metering Infrastructure (AMI) components,
- Communication technology used in the process control domain, e.g., networks, telemetry, telecontrol applications and remote-control technology.
- Energy management systems, e.g., of Distributed Energy Resources (DER), electric charging infrastructures.
- Any Owner of the premises housing the above-mentioned equipment and systems.

## 4. References for Implementation Guidance

The following documents, in whole or in part, are normatively and informatively referenced in ATC (Level 3).

## 4.1 Normative References

4.1.1. IEC/ISA 62443-2-1, Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program.

4.1.2. IEC 62443-3-3, Industrial communication networks – Network and system security – Part 3-3: System security requirements and security assurance levels.

4.1.3. IEC 62443-3-2, Industrial communication networks – Network and system security – Part 3-2: Target security assurance levels for zones and conduits

## 4.2 Informative References

4.2.1. IEC/ISA 62443-1-1, Industrial communication networks – Network and system security –Part 1-1: Terminology, concepts and models.

4.2.2. IEC/TR 62443-2-3, Industrial communication networks – Network and system security – Part 2-3: Patch management in the IACS environment

4.2.3. IEC/TR 62443-3-1, Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems

4.2.4. NIST Special Publication NIST SP 800-82r3 Guide to Operational Technology (OT) Security.

## 5. Document Structure and Approach

The remainder of the Additional Technical Criteria document is divided into the following major Clauses:

5.1 Clause 1 refers to para 7, provides an overview of the cybersecurity management system for the control system, emphasizing special considerations when formulating such a system. It underscores the need to establish a business rationale for integrating the CSMS into the business purpose.

5.2 Clause 2 refers to para 8, outlines the rationale and requirements for the CSMS policy and procedures tailored for the control system. This includes:

5.2.1 Developing Scope

5.2.2 Requirements for Risk Assessment and Risk Tolerance

5.2.3 The necessity and Requirement of a Change Management Policy, Patch Management Policy, Incident Response Plan, Business continuity Plan and system requirements specific to the control system environment

5.2.4 Outlining Risk Management Procedures and Zone & Conduit Requirements.

5.3 Clause 3 refers to para 9, addresses Conformance with the CSMS and the requirement for Monitoring and Continually Improving the CSMS for the Control System.

5.4 Annex A lists the Zone and Conduit requirements mentioned in para 8.14.4 of this section.

5.5 Annex B lists the Control System Security Requirements mentioned in para 8.13.1 of this section.

5.6 Annex C lists the Patch Management requirements mentioned in para 8.10.3 of this section.

## 6. Basic Approach

6.1 To assure security of control system, the requirements prescribed in IEC 62443-3-3 are taken as reference and used as 'system security requirements.

6.2 A security program has been established and is being operated in accordance with IEC 62443-2-1.

6.3 The patch management is implemented consistently as per the recommendation detailed in IEC / TR 62443-2-3.

6.4 The use of IEC 62443-3-2 which describes how a project defines risk-based Security Levels (SLs) which then are used to select the product with the appropriate technical security capabilities.

6.5 For harmonisation with IEC 62443 series of standard, the terms IACS and ICS are used interchangeably. Similarly, the term 'Responsible Entity' has been introduced to harmonise with requirements of CEA regulation.

## 7. Clause 1: CSMS program for Industrial Control System

CSMS program for control system is an enhancement of CSMS requirements defined in BTC L1 and STC L2 to address the issues specific to control system environment as prescribed in IEC 62443-2-1.

### 7.1 Business Rationale

7.1.1 Establishing a robust business rationale for control system cybersecurity management is necessary to secure top leadership support, commitment, and resource allocation for program development, implementation, and maintenance. The first step in the control system cybersecurity program is to outline business objectives and missions. It is essential to comprehend how the control system cybersecurity program can mitigate risks and ensure the secure fulfilment of the utility's objectives and missions. This initial phase is crucial for creating a solid foundation and developing a comprehensive cybersecurity strategy that aligns with the business purpose. The business rationale should encompass the business considerations of top management, illustrating the business impact and financial justification that emphasize the necessity of establishing a thorough cybersecurity program for the control system.

7.1.2 Given the potential gravity of consequences resulting from cyber-attacks, the establishment and execution of a robust Cyber Security Management System becomes imperative. Such a system is not only pivotal for safeguarding critical infrastructure but also for ensuring the safety of individuals, environmental protection, and upholding the utility's reputation and sustainability.

7.1.3 Requirement

The utility is required to formulate a comprehensive business rationale at a strategic level, serving as the foundation for establishing, implementing, maintaining, and continually improving control system cybersecurity. The rationale shall acknowledge and

address the utility's dependence on ensuring the cybersecurity of the control system for its business purposes.

## 8. Clause 2: CSMS Policies and Procedure

8.1 Cybersecurity policies and procedures specific to the control system environment should be formulated by leveraging existing high-level policies, identified risks, and management-defined risk tolerance levels. These documented policies and procedures must be designed to provide clarity for employees, service provider, third parties, and other stakeholders, enabling them to understand the utility's position on cybersecurity and their respective roles and responsibilities in safeguarding the company's assets.

8.2 The communication of these cybersecurity policies and procedures is crucial and should reach all relevant personnel. The utility is responsible for developing and approving cybersecurity procedures that align with the cybersecurity policies. Additionally, it should provide guidance on how to effectively adhere to these policies.

8.3 Requirement

The utility shall develop and maintain a documented cybersecurity policy specifically tailored for the control system environment. This policy shall undergo periodic reviews to ensure its currency, adherence, and relevance. The cybersecurity policies and procedures must encompass applicable regulatory requirements.

### 8.4 CSMS Scope

8.4.1 The utility requires a comprehensive understanding of the operational boundaries and applicability of the control system. Developing a precisely defined scope is pivotal, as it enables management to effectively communicate the objectives and purposes of the Cyber Security Management System (CSMS). It is imperative for the top management to comprehend the delineations within which the CSMS is applicable to the utility, thus establishing a clear direction and focus.

8.4.2 The scope should encompass all aspects of the Control System, including integration points with business partners, customers, and suppliers. The comprehensive scope of work for control system cybersecurity needs clarification from three perspectives: business, architectural, and functional.

a. From a business viewpoint, the scope should define which business units, geographical regions, and specific sites are included.

b. On the architectural front, the scope must detail the inclusion of core control systems, networks, monitoring systems and associated non-production-related systems and its interfaces connections and dependency to external systems including suppliers and customers.

c. In terms of functionality, the functional scope, considerations include how it relates to existing risk management systems, aligns with cyber security policies, conforms to technical standards.

8.4.3 Requirements

The utility shall establish a documented scope for cyber security management system for control system by clearly determining its boundaries and applicability. The CSMS scope must incorporate the strategic goals and processes while specifying the associated timelines and schedules.

### 8.5 Risk Identification, Classification and Assessment

8.5.1 Once the scope is established, an initial risk assessment of the control system should be conducted. This assessment is essential to grasp the financial and HSE consequences that may arise in the event of a compromise in the availability, integrity, or confidentiality of the control system.

8.5.2 Requirements

a. Select a risk assessment methodology: The utility shall identify and list all control system hardware and software components. Furthermore, the utility must establish criteria and assign a priority rating for mitigating the risks associated with each control system component.

b. Provide risk assessment background information: The utility shall identify and list all control system hardware and software components. Furthermore, the utility must establish criteria and assign a priority rating for mitigating the risks associated with each control system component.

c. Conduct a high-level risk assessment: The utility shall perform a comprehensive vulnerability assessment for each specific logical control system. This assessment should be tailored to the results of the high-level risk assessment and prioritize control systems based on identified risks. It is essential to maintain up-to-date records of vulnerability assessments for all assets within the control system.

d. Identify the control system elements: The utility is required to conduct a comprehensive risk assessment that incorporates the vulnerabilities identified in the detailed vulnerability assessment. The results of physical, HSE, and cybersecurity risk assessments shall be integrated to understand the overall risk of the assets. The methodology and results of the risk assessment must be documented.

e. Develop simple network diagrams: The utility shall develop simple network diagrams for each of the logically integrated systems showing the major devices, network types and general locations of the equipment.

f. Prioritize systems: The utility shall develop the criteria and assign a priority rating for mitigating the risk of each logical control system.

g. Perform a detailed vulnerability assessment: The utility shall perform a detailed vulnerability assessment of its individual logical control system, which may be scoped based on the high-level risk assessment results and prioritization of system subject to these risks.

h. Identify a detailed risk assessment methodology: The utility's risk assessment methodology shall include methods for prioritizing detailed vulnerabilities identified in the detailed vulnerability assessment.

i. Conduct a detailed risk assessment: The utility shall conduct a detailed risk assessment incorporating the vulnerabilities identified in the detailed vulnerability assessment.

j. Identify the reassessment frequency and triggering criteria: The utility shall identify the risk and vulnerability reassessment frequency as well as any reassessment triggering criteria based on technology, utility, or industrial operation changes.

k. Integrate physical, HSE and cyber security risk assessment results: The results of physical, HSE and cyber security risk assessments shall be integrated to understand the assets' overall risk.

l. Conduct risk assessments throughout the lifecycle of the control system: Risk assessments shall be conducted through all stages of the technology lifecycle including development, implementation, changes and retirement.

m. Document the risk assessment: The risk assessment methodology and the results of the risk assessment shall be documented.

n. Maintain vulnerability assessment records: Up-to-date vulnerability assessment records should be maintained for all assets comprising the control system.

## 8.6 Risk Tolerance

8.6.1 Establishing and documenting risk tolerance is a crucial step in developing a robust risk management framework, particularly for utilities operating in sectors where public safety and critical infrastructure are paramount.

8.6.2 A periodic review of the utility's risk tolerance is essential, especially when significant changes occur in the utility, technology, business objectives, or due to internal and external events, including identified threats and shifts in the social climate.

8.6.3 Requirements
The utility is required to assess and document its risk tolerance as a foundation for developing policies and conducting risk management activities.

## 8.7 Risk Management and Implementation

8.7.1 Each control system introduces distinct risks to the utility, depending upon the exposed threats, the probability of these threats materializing, inherent vulnerabilities within the system, and the potential consequences of a system compromise.

8.7.2 The risk management outlined in this document necessitates the assessment of risks associated with a particular control system. It involves identifying and implementing security countermeasures to mitigate these risks to an acceptable level. A fundamental concept integral to meeting the mandated risk management requirements is the application of security zones and conduits.

8.7.3 The risk management for control systems establishes requirements for:

a. Defining a System Under Consideration (SUC) for the control system.
b. Partitioning the SUC into zones and conduits.
c. Evaluating the risk for each zone and conduit.

d. Establishing the target security level (SL-T) for each zone and conduit.
e. Documenting the security requirements.

These requirements are derived from IEC/ISA 62443-3-2 and are referred to as zone and conduit requirements (ZCR). The reference standard also offers rationale and supplementary guidance for each mandated requirement.

8.7.4 Requirements: Refer to Annex A: Zone, Conduit and Risk Assessment Requirements

## 8.8 Control System Requirements

8.8.1 The utility should analyse the detailed risk assessment and the impacts on system operations, including business purposes, functions, and reputation, as well as assets, individuals and other dependent organizations. It should prioritize the selection of requirements, focusing on mitigating risks with the greatest potential impact. The implementation of security requirements should be consistent with enterprise architecture and cybersecurity architecture.

8.8.2 Requirement: Annex B lists the mandated Control System Security Requirements

The requirements to mitigate a specific risk may vary among types of control systems. For example, identification and authentication requirements might differ between a control system deployed for an electricity generation plant's Distributed Control System and one for electricity load dispatch SCADA systems. The utility shall identify, evaluate, and implement suitable system requirements to reduce security risks to an acceptable level.

## 8.9 Change Management in Control System Environment

8.9.1 In basic technical criteria documents and supplementary technical criteria documents, utilities have been directed to ensure a change management policy and procedure are established at a high-level structure within the enterprise. Additionally, a formal change management program should be established, with procedures in place to ensure that all modifications to the control system meet the necessary security requirements.

8.9.2 Control systems are complex and often interconnected systems that control critical processes in industries such as power generation, transmission, and distribution. Any changes to the system, whether in software, hardware, or configurations, can potentially introduce instability or disruptions. Proper change management ensures that changes are carefully planned, tested, and implemented to maintain system stability and reliability.

### 8.9.3 Requirements

The utility shall have a defined and documented change management policy and procedure to ensure that all modifications to a control system meet or exceed the identified security requirements of the original components. A risk assessment shall be conducted before implementing any changes to the control system that could impact the system's security, availability, and safety. The current control system configuration must always be known and documented.

**Note**: Introducing changes without proper management increases the risk of vulnerabilities and can create opportunities for unauthorized access or manipulation. Change management is essential for identifying potential risks associated with changes and implementing measures to mitigate those risks.
Where applicable, change management processes shall ensure compliance with legal, statutory, and contractual requirements. This is particularly crucial in sectors where safety, environmental impact, and public welfare are major concerns.

8.10 **Patch Management in Control System Environment**

8.10.1 A documented, defined, and established patch management process for control systems is crucial for maintaining availability, safety, reliability, and security. Control system-specific patch management is a proactive measure to safeguard these systems against vulnerabilities and potential adversarial threats, thus minimizing risks and optimizing performance and resilience.

8.10.2 In a control system environment, patch installations are often scheduled during routine maintenance or outages to minimize operational disruptions. An established patch management process shall help the utility plan and time these installations strategically, ensuring minimal impact on regular operations, as any unplanned changes, including patches, can have profound safety, operability, and reliability implications.

8.10.3 **Requirements**

Annex C: Patch Management in the Control System Environment.

**Note: Obsolete Control System Components and Patch Management:**
The longevity of control systems, often in production for decades, presents a unique challenge, where utilities may have obsolete system for which patching is no longer feasible due to the lack of supplier support and there is reported vulnerabilities, in these cases, a distinct and comprehensive approach is essential to mitigate security risks and protect critical infrastructure. The suggested approach should include Asset Prioritization, network Segmentation and Isolation, enforcing stringent access controls, deployment of Intrusion Detection and Prevention, OS and application Hardening and Whitelisting along with enhanced Logging and Monitoring etc among others. This approach is vital for safeguarding critical infrastructure and ensuring the resilience of utility operations.

## 8.11 Incident Response Plan

8.11.1 The Incident Response Plan enables the utility to proactively prepare for security incidents and respond according to established practices. When developing an incident planning and response program, it is crucial to include all control systems within scope. The incident response plan should outline procedures for how the utility will respond to incidents that is identified or reported in control system environment, covering notification, documentation methods, investigations, recoveries, and subsequent follow-up practices.

8.11.2 Upon identification of an incident, the utility must promptly respond in line with established procedures. Procedures should be in place to identify both failed and successful cybersecurity breaches.

8.11.3 The details of an identified incident should be thoroughly documented to capture the incident, response, lessons learned, and any actions taken to modify the CSMS in response to the incident.

### 8.11.4 Requirements

The utility shall define and implement an incident response plan specifically tailored for the control system environment. This plan shall identify responsible personnel and outline actions to be taken to ensure timely restoration, uphold business continuity, and manage health, safety, and environmental (HSE) impacts.

## 8.12 Business Continuity Plan

A business continuity plan must outline recovery objectives for systems and subsystems, aligning with typical business requirements. It should include a catalogue of potential interruptions and corresponding recovery procedures, along with a schedule to assess part or all of the recovery processes. The utility needs to assess the impact on each system in the event of a significant disruption and determine the consequences linked to the loss of one or more systems. Procedures for maintaining or re-establishing essential business operations during recovery from a significant disruption should be identified.

### 8.12.1 Requirement

The utility shall develop and implement a business continuity plan to ensure the restoration of business processes in accordance with recovery objectives. These plans shall clearly define assigned roles and responsibilities. The utility is responsible for establishing backup and restore procedures that align with the business continuity plan. Regular evaluations of the business continuity plan must be conducted, and updates shall be made as needed.

## 8.13 Control System Security Requirements

The utility should analyse the detailed risk assessment and the impacts on system operations, including business purposes, functions, and reputation, as well as assets, individuals and other dependent organizations. It should prioritize the selection of requirements, focusing on mitigating risks with the greatest potential impact. The

implementation of security requirements should be consistent with enterprise architecture and cybersecurity architecture.

8.13.1 **Requirement**

The Annex B of this Section lists the mandated Control System Security Requirements.

The requirements to mitigate a specific risk may vary among types of control systems. For example, identification and authentication requirements might differ between a control system deployed for an electricity generation plant's Distributed Control System and one for electricity load dispatch SCADA systems. The utility shall identify, evaluate, and implement suitable system requirements to reduce security risks to an acceptable level.

8.14 **Risk Management and Implementation**

8.14.1 Each control system introduces distinct risks to the utility, depending upon the exposed threats, the probability of these threats materializing, inherent vulnerabilities within the system, and the potential consequences of a system compromise.

8.14.2 The risk management outlined in this document necessitates the assessment of risks associated with a particular control system. It involves identifying and implementing security countermeasures to mitigate these risks to an acceptable level. A fundamental concept integral to meeting the mandated risk management requirements is the application of security zones and conduits.

8.14.3 The risk management for control systems establishes requirements for:

a. Defining a System Under Consideration (SUC) for the control system.
b. Partitioning the SUC into zones and conduits.
c. Evaluating the risk for each zone and conduit.
d. Establishing the target security level (SL-T) for each zone and conduit.
e. Documenting the security requirements.

These requirements are derived from IEC/ISA 62443-3-2 and are referred to as zone and conduit requirements (ZCR). The reference standard also offers rationale and supplementary guidance for each mandated requirement.

8.14.4 **Requirements**

Annex A: Zone, Conduit and Risk Assessment Requirements.

## 9. Clause 3: Review improve and maintain the CSMS

9.1 Conformance

Conformance with a CSMS means the Utility is adhering to its stated policies, executing the procedures at the correct time, and producing the appropriate reports to allow for future review. The conformance audit program should delineate the methodology of the audit process. A list of documents and reports needed to establish an audit trail should be developed. The CSMS should include periodic audits of the control system to validate that security policies and procedures are functioning as intended and meeting security objectives.

9.2 Regular

The utility shall conduct periodic audits to validate that the control system adheres to the CSMS, and security policies and procedures are operating as intended. The utility shall define performance indicators to monitor conformance to the CSMS. All the documents and reports required to establish the audit trail shall be maintained as necessary.

9.3 Review, improve and maintain the CSMS

Regular review and monitoring are essential for maintaining the effectiveness of the CSMS, as it needs to adapt to changes in internal and external threats, vulnerabilities, consequences, risk tolerance, legal requirements, and evolving technical and non-technical approaches to risk mitigation. The ongoing process of reviewing, improving, and maintaining the CSMS establishes continuous oversight to ensure its effective functioning and to manage necessary changes over time.

**9.4 Requirement**

| SL | Description | Requirement |
|---|---|---|
| **1** | Evaluate the CSMS periodically | The utility shall evaluate the CSMS periodically or when significant changes are proposed or occur to ensure the security objectives are being met. |
| **2** | Continual improvement | The utility shall continually improve the suitability, adequacy, and effectiveness of the CSMS. |
| **3** | Monitor and evaluate applicable legislation relevant to cyber security | The utility shall identify and evaluate legislations relevant to cyber security for their applicability |

**Annexure A**

**Zone & Conduit Requirements**
**(List the Risk Management and Implementation Requirements of para 8.14.4 of this section)**

1. The Annex A is derived from IEC/ISA 62443-3-2 and describes the requirements for partitioning an SUC into zones and conduits as well as the requirements for assessing the cyber security risk and determining the Target Security Level (SL-T) for each defined zone and conduit. These requirements are referred to as zone and conduit requirements (ZCR).

2. Clause 4 of the standard IEC/ISA 62443-3-2 also provides rationale and supplemental guidance on each of these requirements.

**3. Table-C.1 List of Requirements**

| SL | Steps | Sub steps | Requirement/Considerations |
|---|---|---|---|
| 1 | ZCR 1: Identify the SUC | ZCR 1.1: Identify the SUC perimeter and access points | The organisation shall clearly identify the SUC, including clear demarcation of the security perimeter and identification of all access points to the SUC. |
| 2 | ZCR 2: Initial cyber security risk assessment | ZCR 2.1: Perform initial cyber security risk assessment | The organisation shall perform a cyber-security risk assessment of the SUC or confirm a previous initial cyber security risk assessment is still applicable in order to identify the worst case unmitigated cyber security risk that could result from the interference with, breach or disruption of, or disablement of mission critical IACS operations. |
| 3 | ZCR 3: Partition the SUC into zones and conduits | ZCR 3.1: Establish zones and conduits | The organization shall group IACS and related assets into zones or conduits as determined by risk. Grouping shall be based upon the results of the initial cyber security risk assessment or other criteria, such as criticality of assets, operational function, physical or logical location, required access (for example, least privilege principles) or responsible organization. |
| 4 | ZCR 3: Partition the SUC into zones and conduits | ZCR 3.2: Separate business and IACS assets | IACS assets shall be grouped into zones that are logically or physically separated from business or enterprise system assets. |

| SL | Steps | Sub steps | Requirement/Considerations |
|---|---|---|---|
| 5 | ZCR 3: Partition the SUC into zones and conduits | ZCR 3.3: Separate safety related assets | Safety related IACS assets shall be grouped into zones that are logically or physically separated from zones with non-safety related IACS assets. However, if they cannot be separated, the entire zone shall be identified as a safety related zone. |
| 6 | ZCR 3: Partition the SUC into zones and conduits | ZCR 3.4: Separate temporarily connected devices | Devices that are permitted to make temporary connections to the SUC should be grouped into a separate zone or zones from assets that are intended to be permanently connected to the IACS. |
| 7 | ZCR 3: Partition the SUC into zones and conduits | ZCR 3.5: Separate wireless devices | Wireless devices should be in one or more zones that are separated from wired devices. |
| 8 | ZCR 3: Partition the SUC into zones and conduits | ZCR 3.6: Separate devices connected via external networks | Devices that are permitted to make connections to the SUC via networks external to the SUC should be grouped into a separate zone or zones. |
| 9 | ZCR 4: Risk comparison | ZCR 4.1: Compare initial risk to tolerable risk | The initial risk determined in 4.3 shall be compared to the organization's tolerable risk. If the initial risk exceeds the tolerable risk, the organization shall perform a detailed cyber security risk assessment as defined in 4.6. |
| 10 | ZCR 5: Perform a detailed cyber security risk assessment | ZCR 5.1: Identify threats | A list of the threats that could affect the assets contained within the zone or conduit shall be developed. |
| 11 | ZCR 5: Perform a detailed cyber security risk assessment | ZCR 5.2: Identify vulnerabilities | The zone or conduit shall be analysed in order to identify and document the known vulnerabilities associated with the assets contained within the zone or conduit including the access points. |
| 12 | ZCR 5: Perform a detailed cyber security risk assessment | ZCR 5.3: Determine consequence and impact | Each threat scenario shall be evaluated to determine the consequence and the impact should the threat be realized. Consequences should be documented in terms of the worst-case impact on risk areas such as personnel safety, financial loss, business interruption and environment. |
| 13 | ZCR 5: Perform a detailed cyber security risk | ZCR 5.4: Determine unmitigated | Each threat shall be evaluated to determine the unmitigated likelihood. This is the likelihood that the threat will materialize. |

| SL | Steps | Sub steps | Requirement/Considerations |
|---|---|---|---|
| 14 | ZCR 5: Perform a detailed cyber security risk assessment | ZCR 5.5: Determine unmitigated cyber security risk | The unmitigated cyber security risk for each threat shall be determined by combining the impact measure determined in 4.6.4, and the unmitigated likelihood measure determined in 4.6.5. |
| 15 | ZCR 5: Perform a detailed cyber security risk assessment | ZCR 5.6: Determine SL-T | A SL-T shall be established for each security zone or conduit. |
| 16 | ZCR 5: Perform a detailed cyber security risk assessment | ZCR 5.7: Compare unmitigated risk with tolerable risk | The unmitigated risk determined for each threat identified in 4.6.6, shall be compared to the organisation's tolerable risk. If the unmitigated risk exceeds the tolerable risk, the organisation shall determine whether to accept, transfer or mitigate the risk. To mitigate the risk, continue to evaluate the threat by completing 4.6.9 through 4.6.13. Otherwise, the organization may document the results in 4.6.14 and proceed to the next threat. |
| 17 | ZCR 5: Perform a detailed cyber security risk assessment | ZCR 5.8: Identify and evaluate existing countermeasures | Existing countermeasures in the SUC shall be identified and evaluated to determine the effectiveness of the countermeasures to reduce the likelihood or impact. |
| 18 | ZCR 5: Perform a detailed cyber security risk assessment | ZCR 5.9: Reevaluate likelihood and impact | The likelihood and impact shall be re-evaluated considering the countermeasures and their effectiveness. |
| 19 | ZCR 5: Perform a detailed cyber security risk assessment | ZCR 5.10: Determine residual risk | The residual risk for each threat identified in 4.6.2, shall be determined by combining the mitigated likelihood measure and mitigated impact values determined in 4.6.10 |
| 20 | ZCR 5: Perform a detailed cyber security risk assessment | ZCR 5.11: Compare residual risk with tolerable risk | The residual risk determined for each threat identified in 4.6.2, ZCR 5.1: Identify threats, shall be compared to the organisation's tolerable risk. If the residual risk exceeds the tolerable risk, the organisation shall determine if the residual risk will be accepted, transferred or mitigated based upon the organisation's policy. |

| SL | Steps | Sub steps | Requirement/Considerations |
|---|---|---|---|
| 21 | ZCR 5: Perform a detailed cyber security risk assessment | ZCR 5.12: Identify additional cyber security countermeasures | Additional cyber security countermeasures such as technical, administrative or procedural controls shall be identified to mitigate the risks where the residual risk exceeds the organisation's tolerable risk unless the organisation has elected to tolerate or transfer the risk. |
| 22 | ZCR 5: Perform a detailed cyber security risk assessment | ZCR 5.13: Document and communicate results | The results of the detailed cyber risk assessment shall be documented, reported and made available to the appropriate stakeholders in the organization. Appropriate information security classification shall be assigned to protect the confidentiality of the documentation. Documentation shall include the date each session was conducted as well as the names and titles of the participants. Documentation that was instrumental in performing the cyber risk assessment (such as, system architecture diagrams, PHAs, vulnerability assessments, gap assessments and sources of threat information) shall be recorded and archived along with the cyber risk assessment. |
| 23 | ZCR 6: Document cyber security requirements, assumptions and constraints | ZCR 6.1: Cyber security requirements specification | A cyber security requirements specification (CRS) shall be created to document mandatory security countermeasures of the SUC based on the outcome of the detailed risk assessment as well as general security requirements based upon company or site-specific policies, standards and relevant regulations. |
| 24 | ZCR 6: Document cyber security requirements, assumptions and constraints | ZCR 6.2: SUC description | A high-level description and depiction of the SUC shall be included in the CRS. At a minimum, the CRS shall include the name, a high-level description of the function and the intended usage of the SUC, as well as, a description of the equipment or process under control. |
| 25 | ZCR 6: Document cyber security requirements, assumptions and constraints | ZCR 6.3: Zone and conduit drawings | The organisation shall: a) Produce a drawing or a set of drawings that illustrates the zone and conduit partitioning of the entire SUC. b) Assign each asset in the SUC to a zone or a conduit. |

| SL | Steps | Sub steps | Requirement/Considerations |
|---|---|---|---|
| 26 | ZCR 6: Document cyber security requirements, assumptions and constraints | ZCR 6.4: Zone and conduit characteristics | The following items shall be identified and documented for each defined zone and conduit: a) Name and/or unique identifier; b) Accountable organization(s); c) Definition of logical boundary; d) Definition of physical boundary, if applicable; e) Safety designation; f) List of all logical access points; g) List of all physical access points; h) List of data flows associated with each access point; i) Connected zones or conduits; j) List of assets and their classification, criticality and business value; k) SL-T; l) Applicable security requirements; m) Applicable security policies; and n) Assumptions and external dependencies. |
| 27 | ZCR 6: Document cyber security requirements, assumptions and constraints | ZCR 6.5: Operating environment assumptions | The CRS shall identify and document the physical and logical environment in which the SUC is located or planned to be located. |
| 28 | ZCR 6: Document cyber security requirements, assumptions and constraints | ZCR 6.6: Threat environment | The CRS shall include a description of the threat environment that impacts the SUC. The description shall include the source(s) of threat intelligence and include both current and emerging threats. |
| 29 | ZCR 6: Document cyber security requirements, assumptions and constraints | ZCR 6.7: Organizational security policies | Security countermeasures and features that implement the organisational security policies shall be included in the CRS. |
| 30 | ZCR 6: Document cyber security requirements, assumptions and constraints | ZCR 6.8: Tolerable risk | The organisation's tolerable risk for the SUC shall be included in the CRS. |
| 31 | ZCR 6: Document cyber security requirements, assumptions and constraints | ZCR 6.9: Regulatory requirements | Any relevant cyber security regulatory requirements that apply to the SUC shall be included in the CRS. |
| 32 | ZCR 7: Asset owner approval | ZCR 7.1: Attain asset owner approval | Asset owner management who are accountable for the safety, integrity and reliability of the process controlled by the SUC shall review and approve the results of the risk assessment |

**Annexure B**

**System Security Requirements**
**(List the Control System Security requirements of para 8.13.1 of this section)**

## 1. Security Level

1.1 The IEC/ISA 62443-3-3 standard expands the seven Foundational Requirements (FRs) defined in IEC/ISA 62443-1-1 into a series of Control System Requirements (SRs). Each SR comprises a baseline requirement and zero or more Requirement Enhancements (REs). These baseline requirements and REs are then mapped to the Security Level for the Control System Capability Security Levels (SL-C), ranging from 1 to 4. The defined set of four SLs for all seven FRs allows for an incremental increase in overall control system security, enabling specific components or systems to be configured to protect against progressively complex threats.

1.2 The IEC 62443 series establishes SLs across five levels (0, 1, 2, 3, and 4), each representing an ascending degree of security:

| | |
|---|---|
| 1. SL 0: | No specific requirements or security protection necessary, implying a failure to meet SL 1 requirements for a particular FR within SL-C. |
| 2. SL 1: | Protection against casual or coincidental violations, often resulting from the lax application of security policies. |
| 3. SL 2: | Protection against intentional violation using simple means with low resources, generic skills, and low motivation. |
| 4. SL 3: | Protection against intentional violation using sophisticated means with moderate resources, IACS-specific skills, and moderate motivation, requiring advanced security and domain knowledge. |
| 5. SL 4: | Protection against intentional violation using sophisticated means with extended resources, IACS-specific skills, and high motivation, involving high-performance computing resources or extended periods of time. |

## 2. Control System Requirements Selection Criteria

2.1 The development of control system requirements in this section within ATC (Level 3) is based on the control system requirements and requirement enhancements provided in IEC/ISA 62443-3-3. Recognizing that SL 3 and SL 4 offer protections against intentional violations with control system-specific skills, the control system requirements and requirement enhancements outlined for these two SLs, SL 3 and SL 4 serve as the foundation for determining the requirements for additional technical criteria-level 3.

2.2 It is implied that baseline requirements and requirement enhancements listed against SL 1 and SL 2 are already implemented by the utility while conforming to requirement mandated in basic technical criteria-level 1 and supplementary technical criteria-level 2.

2.3 In the event that any baseline requirements and requirement enhancements are not adhered to in CSMS Scheme for BTC (Level 1) and STC (Level 2) documents, the utility is directed to identify such requirements and make the necessary arrangements to implement them before seeking to implement the system requirements and requirement enhancements mandated in ATC (Level 3). This ensures a comprehensive and robust framework for cybersecurity in alignment with the IEC/ISA 62443-3-3 standard.

## 3. Statement of Applicability

3.1 Control system requirements at higher SLss which are SL3 and SL4 of foundational requirements have been included from IEC/ISA 62443-3-3. However, the utility may exclude the higher security level requirement enhancement within the same security requirement number of any foundational requirement to adhere common control system constraints for ensuring Safety, availability, and integrity and with proper justification and subject to approval of Top Management. For example, in Foundational Requirement 1 – Identification and Authentication Control, in Security Requirement SR 1.1 - Human User Identification and Authentication, both requirement enhancements, RE 2 – Multifactor Authentication for Untrusted Networks for achieving SL3 and RE 3 – Multifactor Authentication for All Networks applicable for achieving SL4, have been mandated. However, the utility can exclude the higher requirement enhancement RE 3 – Multifactor Authentication for All Networks for SR 1.1 under FR 1, provided there is a proper justification for adhering to the common control system security constraints as defined in IEC/ISA 62443-3-3 (see 4 Common control system security constraints).

3.2 Utility may also exclude any control system requirements or requirement enhancement if it is not applicable to them with justification. However, the same shall be subject to approval of Top management. For example, the requirement enhancement 1 of SR 2.2, Identify and report unauthorized wireless devices may be excluded with justification, if utility is not deploying/ permitting any wireless devices in its perimeter.

## 4. List of Applicable Control System requirements

| SL | FR | SR NO | RE NO | SRs and REs | REF CL | SL 3 | SL 4 | Requirements |
|---|---|---|---|---|---|---|---|---|
| 1 | FR 1 – Identification and authenticatio n control | SR 1.1 | SR 1.1 RE 2 | SR 1.1 RE 2 – Multifactor authenticatio n for untrusted networks | 5.3. 3.2 | YES | YES | The control system shall provide the capability to employ multifactor authentication for human user access to the control system via an untrusted network. |
| 2 | FR 1 – Identification and | SR 1.1 | SR 1.1 RE 3 | SR 1.1 RE 3 – Multifactor authenticatio | 5.3. 3.3 | | YES | The control system shall provide the capability to employ multifactor |

| SL | FR | SR NO | RE NO | SRs and REs | REF CL | SL 3 | SL 4 | Requirements |
|---|---|---|---|---|---|---|---|---|
| | authentication control | | | n for all networks | | | | authentication for all human user access to the control system. |
| 3 | FR 1 – Identification and authentication control | SR 1.2 | SR 1.2 RE 1 | SR 1.2 RE 1 – Unique identification and authentication | 5.4.3.1 | YES | YES | The control system shall provide the capability to uniquely identify and authenticate all software processes and devices. |
| 4 | FR 1 – Identification and authentication control | SR 1.3 | SR 1.3 RE 1 | SR 1.3 RE 1 – Unified account management | 5.5.3.1 | YES | YES | The control system shall provide the capability to support unified account management. |
| 5 | FR 1 – Identification and authentication control | SR 1.5 | SR 1.5 RE 1 | SR 1.5 RE 1 – Hardware security for software process identity credentials | 5.7.3.1 | YES | YES | For software process and device users, the control system shall provide the capability to protect the relevant authenticators via hardware mechanisms. |
| 6 | FR 1 – Identification and authentication control | SR 1.7 | SR 1.7 RE 1 | SR 1.7 RE 1 – Password generation and lifetime restrictions for human users | 5.9.3.1 | YES | YES | The control system shall provide the capability to prevent any given human user account from reusing a password for a configurable |
| 7 | FR 1 – Identification and authentication control | SR 1.7 | SR 1.7 RE 2 | SR 1.7 RE 2 – Password lifetime restrictions for all users | 5.9.3.2 | | YES | The control system shall provide the capability to enforce password minimum and maximum lifetime restrictions for all users. |
| 8 | FR 1 – Identification and authentication control | SR 1.9 | SR 1.9 RE 1 | SR 1.9 RE 1 – Hardware security for public key authentication | 5.11.3.1 | YES | YES | The control system shall provide the capability to protect the relevant private keys via hardware mechanisms |

| SL | FR | SR NO | RE NO | SRs and REs | REF CL | SL 3 | SL 4 | Requirements |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | according to commonly accepted security industry practices and recommendations. |
| 9 | FR 2-Use control | SR 2.1 | SR 2.1 RE 3 | SR 2.1 RE 3 – Supervisor override | 6.3.3.3 | YES | YES | The control system shall support supervisor manual override of the current human user authorizations for a configurable time or event sequence. |
| 10 | FR 2-Use control | SR 2.1 | SR 2.1 RE 4 | SR 2.1 RE 4 – Dual approval | 6.3.3.4 | | YES | The control system shall support dual approval where an action can result in serious impact on the industrial process. |
| 11 | FR 2-Use control | SR 2.2 | SR 2.2 RE 1 | SR 2.2 RE 1 – Identify and report unauthorized wireless devices | 6.4.3.1 | YES | YES | The control system shall provide the capability to identify and report unauthorized wireless devices transmitting within the control system physical environment |
| 12 | FR 2-Use control | SR 2.3 | SR 2.3 RE 1 | SR 2.3 RE 1 – Enforcement of security status of portable and mobile devices | 6.5.3.1 | YES | YES | The control system shall provide the capability to verify that portable or mobile devices attempting to connect to a zone comply with the security requirements of that zone. |
| 13 | FR 2-Use control | SR 2.4 | SR 2.4 RE 1 | SR 2.4 RE 1 – Mobile code | 6.6.3.1 | YES | YES | The control system shall provide the capability to verify integrity of the |

| SL | FR | SR NO | RE NO | SRs and REs | REF CL | SL 3 | SL 4 | Requirements |
|---|---|---|---|---|---|---|---|---|
| | | | | integrity check | | | | mobile code before allowing code execution. |
| 14 | FR 2-Use control | SR 2.7 | SR 2.7 | SR 2.7 – Concurrent session control | 6.9 | YES | YES | The control system shall provide the capability to limit the number of concurrent sessions per interface for any given user (human, software process or device) to a configurable number of sessions. |
| 15 | FR 2-Use control | SR 2.8 | SR 2.8 RE 1 | SR 2.8 RE 1 – Centrally managed, system-wide audit trail | 6.10 .3.1 | YES | YES | The control system shall provide the capability to centrally manage audit events and to compile audit records from multiple components throughout the control system into a system- wide (logical or physical), time-correlated audit trail. The control system shall provide the capability to export these audit records in industry standard formats for analysis by standard commercial log analysis tools, for example, security information and event management (SIEM). |
| 16 | FR 2-Use control | SR 2.9 | SR 2.9 RE 1 | SR 2.9 RE 1 – Warn when audit record storage capacity | 6.11 .3.1 | YES | YES | The control system shall provide the capability to issue a warning when the allocated audit |

| SL | FR | SR NO | RE NO | SRs and REs | REF CL | SL 3 | SL 4 | Requirements |
|---|---|---|---|---|---|---|---|---|
| | | | | threshold reached | | | | record storage volume reaches a configurable percentage of maximum audit record storage capacity. |
| 17 | FR 2-Use control | SR 2.11 | SR 2.11 RE 1 | SR 2.11 RE 1 – Internal time synchronization | 6.13.3.1 | YES | YES | The control system shall provide the capability to synchronize internal system clocks at a configurable frequency. |
| 18 | FR 2-Use control | SR 2.11 | SR 2.11 RE 2 | SR 2.11 RE 2 – Protection of time source integrity | 6.13.3.2 | | YES | The time source shall be protected from unauthorized alteration and shall cause an audit event upon alteration. |
| 19 | FR 2-Use control | SR 2.12 | SR 2.12 | SR 2.12 – Non-repudiation | 6.14.1 | YES | YES | The control system shall provide the capability to determine whether a given human user took a particular action. |
| 20 | FR 2-Use control | SR 2.12 | SR 2.12 RE 1 | SR 2.12 RE 1 – Non-repudiation for all users | 6.14.3.1 | | YES | The control system shall provide the capability to determine whether a given user (human, software process or device) took a particular action. |
| 21 | FR 3 – System integrity (SI) | SR 3.1 | SR 3.1 RE 1 | SR 3.1 RE 1 – Cryptographic integrity protection | 7.3.3.1 | YES | YES | The control system shall provide the capability to employ cryptographic mechanisms to recognize changes to information during communication. |

| SL | FR | SR NO | RE NO | SRs and REs | REF CL | SL 3 | SL 4 | Requirements |
|---|---|---|---|---|---|---|---|---|
| 22 | FR 3 – System integrity (SI) | SR 3.2 | SR 3.2 RE 2 | SR 3.2 RE 2 – Central management and reporting for malicious code protection | 7.4.3.2 | YES | YES | The control system shall provide the capability to manage malicious code protection mechanisms. |
| 23 | FR 3 – System integrity (SI) | SR 3.3 | SR 3.3 RE 1 | SR 3.3 RE 1 – Automated mechanisms for security functionality verification | 7.5.3.1 | YES | YES | The control system shall provide the capability to employ automated mechanisms to support management of security verification during FAT, SAT and scheduled maintenance. |
| 24 | FR 3 – System integrity (SI) | SR 3.3 | SR 3.3 RE 2 | SR 3.3 RE 2 – Security functionality verification during normal operation | 7.5.3.2 | | YES | The control system shall provide the capability to support verification of the intended operation of security functions during normal operations. |
| 25 | FR 3 – System integrity (SI) | SR 3.4 | SR 3.4 RE 1 | SR 3.4 RE 1 – Automated notification about integrity violations | 7.6.3.1 | YES | YES | The control system shall provide the capability to use automated tools that provide notification to a configurable set of recipients upon discovering discrepancies during integrity verification. |
| 26 | FR 3 – System integrity (SI) | SR 3.8 | SR 3.8 RE 2 | SR 3.8 RE 2 – Unique session ID generation | 7.10.3.2 | YES | YES | The control system shall provide the capability to generate a unique session ID for each session and treat all unexpected session IDs as invalid. |

| SL | FR | SR NO | RE NO | SRs and REs | REF CL | SL 3 | SL 4 | Requirements |
|---|---|---|---|---|---|---|---|---|
| 27 | FR 3 – System integrity (SI) | SR 3.8 | SR 3.8 RE 3 | SR 3.8 RE 3 – Randomness of session IDs | 7.10 .3.3 | | YES | The control system shall provide the capability to generate unique session IDs with commonly accepted sources of randomness. |
| 28 | FR 3 – System integrity (SI) | SR 3.9 | SR 3.9 RE 1 | SR 3.9 RE 1 – Audit records on write-once media | 7.11 .3.1 | | YES | The control system shall provide the capability to produce audit records on hardware-enforced write-once media. |
| 29 | FR 4 – Data confidentiality (DC) | SR 4.1 | SR 4.1 RE 2 | SR 4.1 RE 2 – Protection of confidentiality across zone boundaries | 8.3. 3.2 | | YES | The control system shall provide the capability to protect the confidentiality of information traversing any zone boundary. |
| 30 | FR 4 – Data confidentiality (DC) | SR 4.2 | SR 4.2 RE 1 | SR 4.2 RE 1 – Purging of shared memory resources | 8.4. 3.1 | YES | YES | The control system shall provide the capability to prevent unauthorized and unintended information transfer via volatile shared memory resources. |
| 31 | FR 5 – Restricted data flow (RDF) | SR 5.1 | SR 5.1 RE 2 | SR 5.1 RE 2 – Independence from non-control system networks | 9.3. 3.2 | YES | YES | The control system shall have the capability to provide network services to control system networks, critical or otherwise, without a connection to non-control system networks. |
| 32 | FR 5 – Restricted data flow (RDF) | SR 5.1 | SR 5.1 RE 3 | SR 5.1 RE 3 – Logical and physical isolation of | 9.3. 3.3 | | YES | The control system shall provide the capability to logically and physically isolate |

| SL | FR | SR NO | RE NO | SRs and REs | REF CL | SL 3 | SL 4 | Requirements |
|---|---|---|---|---|---|---|---|---|
| | | | | critical networks | | | | critical control system networks from non-critical control system networks. |
| 33 | FR 5 – Restricted data flow (RDF) | SR 5.2 | SR 5.2 RE 2 | SR 5.2 RE 2 – Island mode | 9.4.3.2 | YES | YES | The control system shall provide the capability to prevent any communication through the control system boundary (also termed island mode). |
| 34 | FR 5 – Restricted data flow (RDF) | SR 5.2 | SR 5.2 RE 3 | SR 5.2 RE 3 – Fail close | 9.4.3.3 | YES | YES | The control system shall provide the capability to prevent any communication through the control system boundary when there is an operational failure of the boundary protection mechanisms (also termed fail close). This 'fail close' functionality shall be designed such that it does not interfere with the operation of a SIS or other safety-related functions. |
| 35 | FR 5 – Restricted data flow (RDF) | SR 5.3 | SR 5.3 RE 1 | SR 5.3 RE 1 – Prohibit all general-purpose person- to-person communications | 9.5.3.1 | YES | YES | The control system shall provide the capability to prevent both transmission and receipt of general-purpose person-to-person messages. |
| 36 | FR 6 – Timely response to events (TRE) | SR 6.1 | SR 6.1 RE 1 | SR 6.1 RE 1 – Programmatic access to audit logs | 10.3.3.1 | YES | YES | The control system shall provide programmatic access to audit records using an |

| SL | FR | SR NO | RE NO | SRs and REs | REF CL | SL 3 | SL 4 | Requirements |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | application programming interface (API). |
| 37 | FR 7 – Resource availability (RA) | SR 7.1 | SR 7.1 RE 2 | SR 7.1 RE 2 – Limit DoS effects to other systems or networks | 11.3.3.2 | YES | YES | The control system shall provide the capability to restrict the ability of all users (humans, software processes and devices) to cause DoS events which affect other control systems or networks. |
| 38 | FR 7 – Resource availability (RA) | SR 7.3 | SR 7.3 RE 2 | SR 7.3 RE 2 – Backup automation | 11.5.3.2 | YES | YES | The control system shall provide the capability to automate the backup function based on a configurable frequency. |
| 39 | FR 7 – Resource availability (RA) | SR 7.6 | SR 7.6 RE 1 | SR 7.6 RE 1 – Machine-readable reporting of current security settings | 11.8.3.1 | YES | YES | The control system shall provide the capability to generate a report listing the currently deployed security settings in a machine-readable format. |

**Annexure C**

## Patch Management Requirements

**(Lists the Patch Management Requirements of para 8.10.3)**

1. A well-structured patch management process is essential to ensure that any changes are meticulously assessed and securely executed to safeguard these critical aspects. When a structured patch management process is put in place, the documentation of subsequent changes becomes more organized and accountable. This enhances traceability and makes it easier to meet audit compliance and regulatory requirements. Asset owners have an implied obligation to uphold the safety, reliability, operability, security and quality of their operations. Achieving cyber security assurance, through patching control assets, is a critical part of that obligation.

2. The following mandated requirements have been derived from IEC/ISA 62443-2-3 and includes some applicable additional requirements. This reference standard also recommends a defined format for the distribution of information about security patches from asset owners to control system product suppliers, a definition of some of the activities associated with the development of the patch information by control system product suppliers and deployment and installation of the patches by asset owners.

| SL | Requirements |
|---|---|
| **1** | Establish and maintain an inventory of all electronic devices associated with the IACS, that may be updated by modification of their functionality, configuration, operation, software, firmware, operating code, etc. These devices should be referred to as ‘updatable’ devices; |
| **2** | Establish and maintain an accurate record of the currently installed versions for each device, called the ‘installed’ version; |
| **3** | Determine on a regular schedule what upgrades and updates are available for each device, called the ‘latest’ version; |
| **4** | Determine on a regular schedule the ‘released versions’ of upgrades and updates which are identified as compatible by the IACS product supplier and meet the asset owners’ standards for ‘updatable’ devices; |
| **5** | Test the installation of IACS patches in a way that accurately reflects the production environment, so as to ensure that the reliability and operability of the IACS is not negatively affected when patches are installed on the IACS in the actual production environment. Patches which have successfully passed these tests are called the ‘authorized patches’; |
| **6** | Schedule authorized, effective patches for installation at the next available opportunity within the constraints of system design (for example, redundancy, fault-tolerance, safety) and operational requirements (for example, unplanned outage, scheduled outage, on process, etc.); |
| **7** | Update records at a planned interval, at least on a quarterly basis, to include for each updateable device: installed versions, authorized versions, effective versions and released versions; |

| SL | Requirements |
|---|---|
| **8** | Identify a planned interval for installation of patches, such as: when patches are available, or at least on an annual basis; |
| **9** | Install patches and/or implement compensating countermeasures to mitigate security vulnerabilities that exist in the IACS. |
| **10** | Utility shall have a documented procedure for safe fallback options in case in the production environment the patch update is not successful. Utility shall have a mechanism to communicate with their OEMs for necessary supports. |
| **11** | Utility shall have the procedure to schedule the tested patches as per the quantum of residual risk and risk tolerance enumerated in their cybersecurity policy. |
| **12** | Utility shall be bound to apply the critical patches within 35 days of scheduled release and inform in the format prescribed by the regulatory agencies and in case of no updation the reasons to be submitted in writing to the regulatory agencies. |
| **13** | Utility shall ensure at the time of delivery of control system, the supplier provides all required documentation describing the software support and patching policy along with the list of all approved and released patches that qualify for applicability and compatibility. |

**SECTION 4**

# CERTIFICATION PROCESS

## 1. Purpose

This document defines the process to be followed by certification bodies operating certification Scheme of Cyber Security Management System (CSMS) as per ATC (Level 3) for power sector, so that various certification bodies can follow harmonised processes enabling equivalency in their results.

## 2. Scope

2.1 The scope of the document covers certification process of CSMS for CSEs having ICS to the requirements covered in ATC (Level 3).

2.2 The scope of this document covers activities by which a certification body determines that a CSE fulfils certification requirements including application, assessment, decision on certification, maintenance of certification and use of Scheme mark.

Note: The Scheme intents to promote CSMS certification as per ATC (Level 3) which will also have a statement of conformance with the requirements of IEC 62443-3-3.

## 3. Objectives

The objectives of this process are to ensure:

3.1 Uniformity in assessing CSEs seeking certification against the CSMS for ATC (Level 3). This includes all stages and associated activities throughout the audit process ensuring that the audit results are reliable in nature

3.2 Adequate control on the audits process are exercised leading to reliability of the audit.

## 4. Roles and Responsibilities of officials of CB

| S. No. | Role | Responsibility |
|---|---|---|
| 1. | Head – Certification Body | • Overall management of Certification Body.<br>• Formation of the Audit Team.<br>• Reports to the Board<br>(The designation can be as per the organisation culture) |
| 2. | Audit Team Leader (CSMS Lead Auditor- ATC (Level 3)) | Responsible for the entire audit process including managing audit programme, conducting audit, audit reporting, audit follow-up and making the final recommendation for certification or otherwise. |
| 3. | CSMS Auditors (ATC (Level 3)) | Responsible for carrying out audit as per task assigned by the team leader. |
| 4. | Technical Experts | Responsible for advising the team leader and CSMS auditors on technical issues during audit pertaining to the requirements specified in ATC (Level 3). |

| | | |
|---|---|---|
| 5. | CB Secretariat | Responsible for coordinating activities during all stages of the audit process and providing necessary support to the audit team. Additionally, responsible for maintaining certification scheme documentation and records. |

## 5. References

### 5.1 Reference Standards

5.1.1 IS/ISO/IEC 27007:2020 - Information security, cyber security and privacy protection — Guidelines for information security management systems auditing.

5.1.2 IS/ISO/IEC 27006:2015 Amendment 1: 2020 - Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems.

5.1.3 IS/ISO/IEC 19011:2018 - Guidance on the management of audit programmes.

## 6. Process

### 6.1 Application for Certification

6.1.1 It is a pre-requisite that CSEs interested to get CSMS certification for ATC (Level 3) from the CB shall submit application form for certification along with the following documents:

a. Policy and Process documentation of CSEs (also termed as applicant) consisting of:

i. CSMS Policy and procedures documents including risk management process.
ii. Statement of Applicability (SOA)

ATC (Level 3) is built over STC (Level 2) There will be a few commonalities between the requirements of these 2 levels. While carrying out Risk Analysis and formulating Risk Treatment Plan, it is necessary to revisit the analysis done at the time of identifying controls. At this point, while formulating SoA (Level 3), it is required that no necessary controls have been omitted and following is documented and approved by management:

- Identify the necessary controls;
- Justification for their inclusion;
- Whether the necessary controls are implemented or not; and
- Justification for excluding any of the controls.

Note: At this stage, it is suggested applicant to revisit its risk analysis process carried out at the time of certification of STC (Level 2). Since the operating environment at Level 3 is focussed on process control system used by energy utilities and energy suppliers, there are fundamental and significant differences w.r.t conventional ICT environment. Due consideration may be given to IEC 62443-2-1, IEC 62443-2-3 and IEC 62443-3-2 to provide the context of industrial control system requirements.

iii. The applicant shall submit the details of design and implementation of compensating countermeasures.

**Note:** In many cases, the components of ICS don't provide the capabilities required to meet a given security level. In such scenarios, the use of compensating security measures, technical outputs can help to facilitate the needed capability. The combination of multiple techniques within a security solution is designed to fulfil such a role.

iv. Scope of certification
It is applied to process control systems used by the energy utility industry for controlling and monitoring the production or generation, transmission, storage and distribution of electric power, and for the control of associated supporting processes.

- Application Fee
- Certification agreement
- Document Review Report (Cross reference matrix)

**Note:** Document Review Report is the outcome of the process of reviewing for adequacy as per the requirements of technical criteria. This is done to ensure that the system (CSMS) is defined adequately and is adhering to the clauses as mentioned in the technical criteria in definition. Generally, it is done using a Cross Reference Matrix (CRR) wherein against each clause of the technical criteria compliance is ensured and a statement to that effect is recorded.

b. Information on use of certified components, sub-systems, and systems

For product suppliers, various CBs provide certification services based on IEC 62443-4-1 - "Secure Product Development Lifecycle". Corresponding certifications are available to system integrators based on IEC 62443-2-4 -"Security Program for Service Providers". Besides the process aspects during product development and system integration, IEC 62443 also specifies technical security requirements for components and systems, which are described in IEC 62443-4-2 and IEC 62443-3-3. This information should be supplied along with application.

c. Information on System Security Capabilities

Applicant shall provide information on system security capability for each of the requirements of Level 3. Refer to the table below for reference:

| S No. | Level 3 requirement | Capability Description |
|---|---|---|
| FR 1<br>1. | Human user identification and authentication | <Model/ID of the sub system> provides contextual identity across both wired and wireless networks.<br><Model/ID of the sub system> provides MFA to connections as needed, such as for added protection for remote-access users. |

6.1.2 Since the certification Scheme is in the maturing phase, at this juncture this scheme does not permit a joint application/audit/certification for BTC (Level 1) and STC (Level 2) and ATC (Level 3). An applicant CSE should follow only step by step approach. However, they can implement BTC (Level 1) and STC (Level 2) criteria concurrently. Any additional explanation needed by the applicant will be provided by the CB, on

receipt of a specific request for the same, including necessary explanations on the specific scopes of certification that are covered.

6.1.3 Before applying for certification, the applicant shall have met the following conditions

a. Operated the CSMS/ISMS (IS/ISO/IEC 27001:2022) as per the certification criteria for at least 1 year. This is necessary to ensure the ability of the applicant to have a stabilised system under normal operating conditions.

*Note: The IS/ISO/IEC 27001:2022 or IS/ISO/IEC 27001:2013 or CSMS BTC (Level 1) and the IS/ISO/IEC 27019:2017 or CSMS STC (Level 2) implementation for one year is considered as compliance to this condition.*

b. Carried out minimum one internal audit against the applicable criteria as per applied scope for certification, one management review for the documented CSMS. Audit of BTC (Level 1), STC (Level 2) and ATC (Level 3) may be done concurrently and sequentially.

6.1.4 The CB appoints a Team Leader (TL) for initiating the certification process.

6.1.5 The application is reviewed by the appointed TL for completeness and obtaining a confidence that the applicant has clarity of certification requirements and the capability of CB to provide the required certification services in timely manner. CB will review its ability to carry out the audit in terms of its own policy and process, its competence and the ability of personnel suitable for audit activities. Any mismatch is clarified and the outcome of the review is communicated to the applicant regarding acceptance of the application for further processing, or for completing any further requirements identified during the review. CB reserves the right to seek information on the antecedents of the owners / those managing CSEs activities and analyse it before deciding to accept the application for further processing. It may decide not to accept application if there is any adverse finding in the above exercise. The decision of the CB shall be communicated to the applicant with reasons for not accepting the application. The applicant can appeal against such a decision.

6.1.6 Upon deciding to accept the application, the same is recorded or registered and the audit team is appointed.

6.1.7 At any point of time during the certification process the applicant may request for transferring the registered application to another legal entity. CB would allow the same without any additional application fees based on the justification provided by the CSEs and subject to the new legal entity meeting all the requirements of application for CB Scheme.

6.1.8 In case the application is accepted for further processing, a formal acknowledgement along with a proposal is sent for carrying out the audit of the applicant based on the expected man-days and fee schedule.

6.1.9 On receipt of acceptance of the proposal from the applicant and the audit fee as per the contract as well as the appointment of the audit team, further processing of application is done.

### 6.2 Appointment of the Audit Team

6.2.1 The audit team, consisting of a TL and the members, is identified by CB from the pool of auditors and experts. The audit team shall include Technical Expert, in addition to the number of team members having knowledge of CSMS Scheme for ATC (Level 3) and related standards.

6.2.2 The names of the members of the audit team for carrying out the document review and the onsite audit are also communicated along with the CV to the applicant along with the proposal and is requested to inform CB about acceptance of or objection against the appointment of any of the team members. Any objection by the applicant against any of the team members must be in writing, accompanied with adequate grounds for the objection. The CB will evaluate the objection and decide whether to change the team member or to overrule the objection raised by the applicant. The audit team is then formally appointed. Efforts are made to ensure that the team is kept intact throughout the initial audit process, however this cannot be guaranteed. The team members are asked to commit that they do not have relationship direct/indirect with the applicant that can affect the objectivity of the audit at the time of their appointment as CB Auditor / expert. The team members are required to maintain confidentiality of the sensitive information about the operation of the applicant obtained as part of the audit process unless required by law, in which case the same will be done under intimation to the applicant. The audit team members shall meet the requirements mentioned in Annex B of Section 5: Requirements for Certification Bodies'.

6.2.3 All CB Auditors needs to declare that they have no conflict of interest and committed to disclose if such a situation arises so that CB can take appropriate decision.

6.2.4 If a preliminary visit is requested by the applicant, the CB Secretariat shall organize the same after obtaining the acceptance of the preliminary visit fee by the applicant. Such a visit would solely be for the purpose of gaining a better understanding of the operations of the applicant and for the applicant to better understand the certification process and clarify the expectations of CB as regards the requirements of the standards. The visit may result in communication of findings to the applicant. Such a visit would not result in any decrease in the man-days for the initial audit.

### 6.3 Certification Requirements

#### 6.3.1 Certification Criteria

The CB shall use the 'Additional Technical Criteria (Level 3)' for CSMS as reference document for carrying out the audit.

#### 6.3.2 Amendment to the Criteria

a. The amendment to the Criteria shall be based on the nature of changes required and approved by QCI (with approval of MSC). The Criteria of certification and any application documents may also be taken up for amendment based on following conditions, individually or severally:

i. Any change in the international standards and guides.
ii. Significant feedback from the Peer Review audit team that warrants amendment.
iii. Significant feedback from the implementation of the criteria.
iv. Any other reason as deemed fit by the QCI.

b. The QCI shall approve the amended criteria after due consultation, if needed, as follows:

i. Seek the advice of the Technical Committee, if one exists,
ii. Seek representation of certification bodies before approval of the amendment.
iii. Seek public comments on the proposed changes through the Members of the Board and other representative bodies as the Board may deem fit.

c. The issue status of the criteria documents is identified by the version no., month and year of the issue.

### 6.4 Conditions for Certification

#### 6.4.1 Granting of Certification

a. The certification is granted to an applicant on completion of audit and after the conditions given below are met with by the applicant:

i. The applicant meets the criteria of certification and all non-conformities and concerns found against the criteria of certification during audit have been closed to the satisfaction of the CB in accordance with the guidelines on the subject.
ii. There are no adverse reports / information / complaints with the CB about the applicant regarding the quality and effectiveness of implementation of CSMS as per the criteria of the CB. There is also no evidence of fraudulent behaviour.
iii. The clients of the CSEs are satisfied by the conduct of the applicant and its CSMS. CB may request feedback from selected clients of the applicant / publicize receipt of application and seek feedback from stakeholders.
iv. The applicant has paid all the outstanding dues.
v. The certification shall be for a period of 3 years.

b. In the event of any adverse issue arising from the reasons specified at points ii. and iii. above, or if there is evidence of fraudulent behaviour or if the applicant intentionally provides false information or conceals information, the applicant will be given an opportunity to explain its position in writing to the CB and present its case in person to the certification committee. The final decision shall be taken in respect of granting of certification on the basis of review of the facts and the results of such presentation.

c. The CSMS scope document should cover all aspects of audit requirements include the following:

i. List of processes and services included in the scope.
ii. List of departments or other organizational units included in the scope.
iii. List of physical locations included in the scope.
iv. Exclusions from the scope.

d. Once organisation fulfils all audit requirements a certificate will be issued by CBs covering certification of ATC (Level 3) and IEC 62443-3-3. A sample of certificate is mentioned below:

Certificate Ref. No.:

___

SAMPLE OF CERTIFICATE

This is to certify that Cyber Security Management System of
<Name of the CSE>
<Address of the CSE>

has been assessed and found to conform to the requirements of
Additional Technical Criteria (Level 3), Version No._____
<Energy utility industry for its system security requirements and applicable security levels based on the principles as defined in IEC 62443-3-3>

SOA Detail: _____
Dated: dd/mm/yyyy

Annexures:

i. List of Industrial Control System and services included in the Scope
ii. List of departments or other organizational units included in the Scope
iii. List of physical locations included in the Scope
iv. Exclusions from the Scope

Authorised signatory
Date of issuance of certificate: dd/mm/yyyy
Valid up to: dd/mm/yyyy
Date of surveillance: dd/mm/yyyy

*******

e. CB shall publish on its website, grant of any new certification, for information and feedback from the industry / other stakeholders.

6.4.2 **Maintaining Certification**

a. The certified CSEs shall comply with the following requirements. Subject to its meeting the conditions given below the certification given to a CSEs shall be maintained for three years.

i. The certified CSEs continues to meet the criteria of certification and all nonconformities found against the criteria of certification during surveillance audits have been closed to the satisfaction of the CB as per laid down criteria.
ii. There are no adverse reports / information / complaint with the CB about the applicant regarding the implementation of CSMS as per the criteria laid down by the CB. There is also no evidence of fraudulent behaviour.
iii. The clients of the CSEs are satisfied by its conduct and its CSMS.
iv. The certified CSEs has organized onsite audit as required by CB.
v. The certified CSEs has paid all the outstanding dues.

### 6.4.3 Suspension of Certification (Partial or full)

The certified CSEs shall be subject to suspension of certification either fully or partially, both in terms of scopes. It shall be based on the following conditions individually or severally.

a. No/ineffective corrective actions in response to the nonconformities observed during surveillance audits or recertification audits.
b. Non-payment of outstanding dues.
c. Not organizing audits in time.
d. Any significant/major changes in the legal status, ownership, impartiality, use of sub-contractors, documentation, etc., which have not been informed to the CB within 30 days.
e. Any wilful misuse of the certification mark of the CB and NABCB.
f. Any wilful mis-declaration in the application form, which is discovered after the grant of certification/ recertification.
g. Wilful non-compliance to the certification agreement.
h. Wilful misuse of certification conditions for scopes not covered under scope of certification.
i. Inability or unwillingness to ensure compliance of the CSEs' CSMS certified by the accredited certification body, to the applicable standards.
j. Fraudulent Behaviour and providing intentionally false information or concealing information.
k. Excessive and or serious complaints against the CSMS of the certified CSEs.
l. Evidence of lack of control over the CSMS process/wilful bypassing of CSMS process.
m. Evidence of unethical practices including providing incorrect information to CB; misrepresentation by sales personnel; faking of CSMS records; etc.
n. Non-availability of resources in some of the technical areas covered under certification.
o. Inability or unwillingness to organize onsite audits due in time.
p. Critical or major non-conformity which may bring into question the CSE organisation's ability to provide service in compliance with the certification norms.
q. Any other condition/situation deemed appropriate by the certification committee:

i. A notice citing reasons and intention to suspend shall be sent to the CSEs inviting response within 15 days.

ii. The CSEs shall be given an opportunity to explain its position in writing to CB and present its case in person to the certification committee. The final decision shall be taken in respect of Suspension of Certification (Partial or full) on the basis or facts and the results of such presentation.

iii. Not with-standing the above provision for a representation by the CSEs, the certification committee may decide to suspend certification if there is sufficient evidence of wilful misrepresentation of facts or wilful non-compliance to certification criteria. The period of suspension shall be formally communicated as per the criteria laid down by the CB.

iv. The information about suspension (partial or full) of the certification of the CII organisation shall be published on CB website for information to all and feedback from the industry / other stakeholders.

### 6.4.4 Withdrawal of Certification

a. The CSEs shall be subject to withdrawal of certification based on the following conditions individually or severally:

i. If an CSEs voluntarily relinquishes its certification status
ii. If the non-conformities are not appropriately addressed in spite of suspension/withholding of recertification for a period not more than six months
iii. If no action is taken by the CSEs in response to the suspension on any other grounds.
iv. Complaints are received about the CSMS/ CSEs and established to be based on facts.
v. Critical or major non-conformity which may bring into question the CSEs' ability to provide service in compliance with the certification norms.
vi. Any serious non-compliance to Terms and Conditions of certification especially any fraudulent behaviour which may warrant withdrawal.
vii. Any other condition/situation deemed appropriate by the certification committee.

b. A notice of the intention to withdraw certification, citing reasons shall be sent to the CSEs, who shall respond within 15 days.

c. The certified CSEs shall be given an opportunity to explain its position in writing to the CB and present its case in person to the certification committee. The final decision shall be taken in respect of withdrawal of certification on the basis of facts and the results of such presentation.

d. The withdrawal of certification shall be formally communicated as per the criteria laid down by the CB.

e. The CB shall publish information about any withdrawal of certification on its website, if necessary for information of the industry / other stakeholders, if required.

### 6.5 Audit

The certification shall be for capability of the CSEs in operating a sound CSMS in compliance with the technical criteria and certification process.

#### 6.5.1 Preparation for the Certification

a. The CB prepares an audit plan for the initial certification process covering two stages as follows:

i. **Audit Stage 1 - Detailed review of the applicant's CSMS documentation:** This shall cover all levels of documents of the CSEs for the certification programme(s) applied for. For this audit, the auditor shall focus on risk management process, Statement of Applicability (SoA) and selection of controls based on results of risk analysis to demonstrate adequacy of the defined system.

ii. **Audit Stage 2: Onsite Audit of the applicant's CSMS:** The on-site audit of the applicant's CSMS including any branch offices / locations from where the CSEs offering its services / sub-contractors, as applicable is carried out.

The normal certification duration for each stage of audit is described at Annex A of this section. The draft audit plan may be prepared in stages as mentioned above depending on the information supplied and as when the audit activity is planned and executed using a risk-based approach. The clarifications regarding the scopes applied for, auditor expertise available with applicant, etc. shall be provided in advance for finalizing audit plan.

iii. For the purpose of assessing scope of certification applied for, the same shall be assessed through combination of means such as documentation review where the CSEs' system for adequate definition its ability to comply with the technical criteria would be reviewed. Then during on-site audit review of records of key activities performed to ensure effective implementation of CSMS. The choice of audit technique will be decided based on risk.

iv. All locations (such as branch/sub-contractor's office) mentioned in the scope of certification shall be audited being the part of CSE.

6.5.2 **Certification Audit plan**

a. Based on the draft certification audit plan, CB Secretariat prepares a detailed schedule for the following stages of the audit.

i. Audit Stage 1 – Adequate definition of CSMS (Detailed review of the applicant's CSMS documentation): Audit of the documentation of the CSEs to ensure CSMS adequately addresses the requirements of Technical Criteria.

ii. Audit Stage 2 – Effective implementation (Onsite Audit of the applicant's CSMS)**:** Onsite Audit of the CSEs including branch offices / locations / subcontractors to ensure compliance with the defined CSMS.

b. The audit TL shall identify the auditors (within the scope of certification) of the CSEs.

6.5.3 **Audit Stage 1 - Detailed review of the applicant's CSMS Documentation**

a. In audit stage 1, the audit team performs a detailed review of the applicant's documentation for ensuring compliance with all applicable requirements of the CSMS standards & certification criteria. Audit stage 1 includes preliminary verification of the organisation's implementation of the process for internal audit and management review. The objectives of audit stage 1 are to gain an understanding of the CSMS in the context of the organisation's security policy and objectives. At this stage, a status review of maintenance of BTC (Level 1) and STC (Level 2) is also performed.

b. The documents shall be verified by the audit team leader / a member of the audit team for compliance to the certification criteria as supported by the application documents and the scope applied for by the applicant. In case the CSEs applies for more than one certification Scheme, then it shall be ensured by having appropriate number of Auditors that at least one Auditor qualified for each certification Scheme is part of the audit team. A document review report of any omissions/deviation of the criteria elements is forwarded by the team leader, to the CSEs for its comments and compliance.

c. Depending on the nature of comments and changes to be made to the documentation, decision regarding a second review of documents shall be taken. The CSEs shall be

informed if a second review is needed. If significant changes are needed the second review may be charged. Any review beyond second document review would be charged by CB.

d. Any further review of documents would be charged to the CSEs. If the documentation does not meet the requirements even after 3rd review, the application is liable to be rejected. In such an event, the decision of the CB shall be communicated to the applicant with reasons for rejecting the application. The applicant can appeal against such a decision.

e. CB may decide to conduct a preliminary visit in case the documentation does not meet requirements after two reviews, to give an opportunity to the CSEs to clearly understand the certification criteria and other requirements. The visit shall be charged to the CSEs and the duration shall be decided by the CB based on the work involved. The preliminary visit will generally be carried out for one-man day by the appointed leader of the audit team that carried out the documentation review.

f. If the documentation is determined to be generally meeting the certification criteria, after review of the changes made, team leader may seek evidence of implementation of changes to the system by the CSEs.

g. Subsequent to the audit stage 1 (documentation review), the Audit Stage 2 - onsite audit of the CSEs, as per the certification audit plan decided at the beginning, shall be planned. The team leader and the team member involved in the documentation review activity shall generally be part of the audit team. Any additional team members may be inducted based on the review of man-days and scope applied for.

### 6.5.4 Audit Stage 2 – Onsite Audit of the applicant's CSMS

a. In audit stage 2, the audit team performs audit of the applicant's CSMS to confirm that the CSEs has implemented the documented CSMS, it adheres to the policies, objectives & process & requirements of CSMS, and by implementing CSMS is achieving the organisation's policy objectives. The objective of audit stage 2 is to verify that CSEs has effectively implanted the documented CSMS.

b. The audit plan for the onsite audits, as prepared by the team leader is shared with the CSEs for their agreement. The responsibility for preparation of audit plan is that of the team leader.

c. The audit team will carry out the audit of the implementation of the CSEs documented system in the head office of the applicant and if necessary, at other office sites / sub-contractors included in the certification application/audit programme.

d. The branch offices / sub-contractors carrying out activities as defined shall be included in the audit programme and shall be covered during certification cycle.

e. During the audit and/or on demand at any time, the applicant / certified CSEs shall provide unrestricted access to the documents and records that pertain to implementation of CSMS in accordance with the certification criteria for the scope applied for. The records shall also include the records pertaining to applicant and clients of the CSEs and the CSMS and the scope applied for. Access shall also to be provided to the records of the complaints and appeals along with corrective actions

and the method of verifying the effectiveness of the corrective actions. Under certain circumstances, where possibility of irregularity, malpractice and/or fraud is suspected, the records under review may also include the financial records as relevant/applicable to the CSMS. Under these circumstances the CB Auditors shall demand and take copies in any form as relevant – hard copies, scanned copies, etc.

f. The non-conformities observed during the onsite audit shall be explained to the CSEs and given in CB designated format for carrying out root cause analysis and proposing corrective actions for preventing recurrence as well as corrections, where applicable, concerns may also be raised. The timelines for the corrective action completion shall be agreed to by the audit team leader and the authorized personnel of the applicant as per the timelines laid down on this aspect.

g. The team leader shall recommend, at this stage, whether to await completion of the corrective actions or to proceed with the on-site audits scheduled to be carried out. Generally, any major NC in respect of areas like capability or CSMS, would require the CSEs to take corrective actions before audit is planned. The Team leader shall send a report to the CSEs and CB, including details of the recommendations for audits and the audit plan, as per the Guidelines of the CB.

h. The team, nominated by CB Secretariat, shall carry out the audit as per the audit plan, based on the scopes applied for. The CB shall ensure that the audit covers the representative processes of the concerned scope sector/technical area. The audit shall cover the complete process of audit for certification.

i. The CB audit team shall identify the findings (non-conformities, concerns, etc.).

j. A meeting shall be held on completion of audit and the applicant shall be explained and provided with, as far as possible, documented copy of the nonconformities/concerns observed during the audit for corrective action as per the guidelines established by the CB. Additional NCs/Concerns may also be raised based on review of other records pertaining to the CSMS documentation & implementation. The team also provides an opportunity for the applicant to ask any question about the findings and its basis during the meeting.

### 6.5.5 **Audit Report**

a. The audit team shall prepare a report at each stage of the audit – audit stage 1 (CSMS documentation review), and audit stage 2 (on-site audits). Nonconformities and Concerns, or list of findings, if any, shall be handed over to the CSEs' representative at the end of each audit. The report at each stage of audit shall be sent by the CB audit team within prescribed timelines. If no comments are received within a week, then the report is considered to be acceptable to the CSEs and is deemed as final.

b. The process of closing the non-conformities/concerns and verification must be completed in the specified time. If the applicant delays the process of acceptable corrective action beyond the limits specified by the CB, the CB will reserve the right to reject the application. The fees paid by such applicant will be forfeited. In such an event, the decision of the CB shall be communicated to the applicant with reasons for rejecting the application. The applicant can appeal against such a decision.

c. After all the preceding steps are over, the final report shall be reviewed for completeness, by the CB, with respect to guidelines on the subject and shall be presented to the certification committee for its decision on the grant of certification to the applicant.

### 6.5.6 Audit findings (Nonconformities/Concerns) and Corrective Actions

The non-conformities observed shall be categorized in three categories:

a. **Critical**

i. Any failure of implementation of the certification criteria and raises doubts on the operation and practice of CSMS and the results.

ii. Any evidence that indicates possibility of fraudulent/irregular behaviour by the CSEs.

iii. Critical non-conformities shall call for the immediate correction and corrective actions based on appropriate root cause analysis. Such actions shall have to be completed and non-conformities addressed within 30 days of the date these have been observed by the audit team as per the established criteria of the CB. Critical NC shall be brought to the immediate notice of CB by the Team Leader (TL) of the CB AT. The CSEs may be liable for suspension/withdrawal of certification with due notice if such NCs are raised even as it takes action to address them. In case the corrective action is not completed within the stipulated time frame, the certification may be liable for suspension partially or completely or withdrawal based on the nature of non-conformity.

b. **Major**

i. Any evidence that casts doubt on the CSMS and is less severe than in case of the critical (which bring into question the validity of certificate issued) and is evident in failure of certain elements of the criteria individually (e.g., risk management or internal audit system not working). It may have less direct impact on the CSMS and its results or any minor non-conformities that have not been acted upon within the stipulated time frame. A number of minor nonconformities associated with the same requirements or issue may be considered as major nonconformity if it indicates a systemic failure.

ii. Major non-conformities shall call for the early correction and corrective actions based on appropriate root cause analysis. Such actions shall be completed, and non-conformities addressed within 60 days of the date these have been observed by the audit team as per the established criteria of the CB. The CSEs shall get 10 days for proposing corrective actions and the CB AT shall get 10 days for review and response on these. In case the corrective actions are accepted, the CSEs shall be given 15 days to submit evidence of the implementation of the accepted corrective actions which the CB AT will review and respond within 15 days. In case the NC is not addressed within the stipulated time frame, the certification may be liable for suspension partially or completely based on the nature of the non-conformity.

c. **Minor**

i. Any evidence that indicates a non-compliance to the certification criteria and the application documents, which has negligible impact on the CSMS and its results.

ii. Minor non-conformities shall need to be addressed and corrected as early as possible, but not later than 3 months from the date these have been observed by the audit team, as per the established criteria of the CB. In case of minor NCs also the CSEs will be required to undertake appropriate root cause analysis before deciding the corrective action. One of the analyses it will require to do is to establish whether it is an isolated case or there are other instances the same finding is observed since the rigour of the corrective actions decided will depend on the same.

iii. CSEs is required to propose corrective actions within 15 days, and the CB AT shall review / respond on proposed CAs within 10 days.

**Note 1:** Multiple Minor NCs with related impact on the CSMS shall result in a Major non-conformity based on the judgement of the audit team.

**Note 2**: NCs remaining unresolved after the prescribed timelines are liable to be upgraded to the next higher category.

d. **Concerns**

The CB audit teams may also raise concerns under the following circumstances:

i. Minor gaps/inadequacies observed, in CSEs' documented system or practices, which do not directly amount to non-compliance. However, if no action is taken, they are likely to result in non-conformities.

ii. Issues observed during audits, which may require further review and audit of the CSMS of the CSEs.

iii. Findings of minor nature where, in the judgement of the audit team, root cause analysis in not required.

iv. Issues from documentation review, minor in nature, which have remained unresolved subsequent to audit, where the practice of the CSEs was observed to be complying with the requirements of the standard.

v. Concerns are findings which do not require the CSEs to carry out any root cause analysis. It can directly inform the correction/corrective actions it has taken or intends to take (where it would take time). In certain cases, where there are unresolved issues from documentation review, the CB AT may ask the CSEs to submit the evidence of Corrective actions for the resolution of the concerns.

e. The CSEs shall be given only two chances/iterations for acceptance of corrective actions (proposed/implemented) and closure of non-conformities/concerns and from 3rd iteration onwards, they would be charged for the additional review accordingly (0.5/1 man-day as decided on case- to case basis).

f. The time for addressing the NCs/Concerns shall be reckoned from the day the nonconformities are handed over to the CSEs.

g. Non-conformities of critical or major nature shall normally call for an onsite follow up as per recommendation of the audit team. Such a follow up visit shall be charged as per prevailing fee structure.

h. In case of minor non-conformities, a declaration in respect of completion of the corrective action by the authorized person of the CSEs may be accepted. However, during surveillance, if it is found that the Minor non-conformity is not effectively addressed, the non-conformity shall be upgraded into major non-conformity and shall have to be treated as per the criteria laid down for Major Non-conformity.

**Note:** The audit team may also identify opportunities for improvement and convey the same to the CB as observations and include in their final report.

6.5.7 **Time Period for audit process**

a. The audit process for any applicant must be completed within a maximum of one year. In the event that the process is not completed within one year, CB will take a decision and the application may then be kept active for one more year and applicant may be given one chance to completely restart the audit process afresh without paying any additional application fee. In such cases the audit process must be completed in one additional year.

b. In the event of delay in scheduling of audits for scope applied for, the applicant may apply in writing to the CB for consideration of his application for part of the scope, for which the audit process as per CB process has been completed. The CB shall have the right to accede to that request or differ. Grant of certification for part of the scopes shall be done subject to completion of Corrective Actions for all the non-Conformities and concerns raised during the earlier stages audits conducted and their acceptance/closure as per the laid down criteria of the CB.

## 6.6 Certification Decision

6.6.1. The Certification Committee is responsible for taking decision on granting, maintaining, extending, reducing, suspending or withdrawing of Certification and also withholding of recertification as well as extension of validity of certification. It also ensures that the members of the Certification Committee were not involved in the audit and also have had no relationship for the last two years with the applicant under consideration that can influence their decision on certification.

6.6.2. The reports are presented to the certification committee along with recommendations of CB for the decision of certification.

6.6.3. The decision of certification is taken by the Certification Committee unanimously and is generally not put on vote. The Head of the Committee shall be responsible for coordinating and addressing the issues raised by the members. The Head of the committee shall have the right to call for any other Auditor/experts/personnel for clarifying any of the issue that is under discussion. The persons so called for clarification shall not take part in the decision of the certification. It shall be ensured that the persons so called for clarifications shall not have taken part in the audit of the concerned applicant and shall be free from any conflict of interest, except when clarification form the audit team is needed.

6.6.4. The decisions of the certification committee are based on the audit report, recommendations of the audit team and the CB, any other relevant information about complaints, the market reputation obtained by the CB, etc. It may also involve interaction with the CB, audit team and the applicant. The certification committee in its capacity shall have the right to ask for any further clarifications on the report and information submitted on the applicant's CSMS and the applicant shall not refuse to present such information.

### 6.7 Certification information / Documents

6.7.1. The certification committee shall decide to grant certification to the applicant, only after the applicant has met all the conditions specified by the CB.

6.7.2. Two copies of the certification agreement shall be signed by the CB and CSEs shall ensure that the relevant fees are paid.

6.7.3. On receipt of the signed agreement and the fee as per the invoice, a set of certification documents shall be issued to the applicant along with the artwork of the certification mark of the Scheme.

6.7.4. The certification "certificate" in the standard template shall include the CB certification symbol, the name of the CSEs, address of the premises of the CSEs from where key activities are performed, certification number, the scope of certification, effective date of grant of certification and the date of expiry or renewal date of the certificate. In addition to this, the following details are also included:

a. Standards/Normative documents and/or regulatory requirements to which organizations are certified including issue or revision used for audit.

b. Name of the Scheme – "Conformity Assessment Framework for CSEs"

6.7.5. The certificate shall be valid for three years and the date of issue and validity is indicated on the certificate.

6.7.6. The Scope of certification granted to a CSEs is indicated on the certificate. Whenever there is a change in scope (extension or reduction) which calls for a revision of the certificate, the certificate will carry the revision no. (such as Rev 1) with a disclaimer as follows: "This certificate supersedes the earlier version of the certificate dated …….". In addition, the CSEs will also be asked to return the earlier version of the certificate and / or schedule.
In case of scope reduction, the revised certificate and / or schedule will be issued only after receipt of earlier version of the certificate and / or schedule from the CSEs.

### 6.8 Maintaining Certification and Certification Cycle

#### 6.8.1. Surveillance Audit

a. To ensure that each certified CSEs continues to comply with the certification requirements, a surveillance audit of CSEs shall be carried out once in 12 months as per the audit programme i.e. before 12 and 24 months. The first surveillance audit shall be carried out within 12 months from the date of grant of certification by a physical visit. However, the certified CSEs, for valid reasons may seek a postponement of the audit for a maximum period of three months. For deferring the surveillance, the CSEs shall give written justification and shall obtain the consent of CB.

b. The surveillance audit shall include locations performing key activities. The number of locations included in the surveillance audit would be based on the risk consideration.

c. Since ATC (Level 3) certification has a prerequisite of continuing complying with the requirements of BTC (Level 1) and STC (Level 2), it is the requirement of the CSE to ensure sustain maintenance of BTC (Level 1) and STC (Level 2) certifications. This is achieved through close liason between the CSEs and CB by conducting timely surveillance audits. If CSEs withdraw BTC (Level 1) or STC (Level 2) certificates or there is a case of suspension of the same, the validity of ATC (Level 3) cease to exist.

d. Surveillance audit for BTC (Level 1), STC (Level 2) and ATC (Level 3) can be combined provided that all experts required are part of the team and collective requirements are factored for man-days calculation.

6.8.2. The non-conformity reports and concerns if any and the audit report of each of the surveillance audits shall be forwarded to the certified CSEs for taking corrective action as per the laid down criteria for the maintenance of certification.

6.8.3. In the event of any critical and/or major non-conformity that can affect the CSMS, the CB informs the certified CSEs and seeks a time bound corrective action plan. The decision for an additional follow up visit to verify the implementation of the corrective action plan as committed by the certified CSEs is taken by the CB in consultation with the Team leader of the audit team. Such decision shall be binding on the certified CSEs. The cost of the follow up visit shall be borne by the certified CSEs. In the event certified CSEs has not shown evidence of completion of the corrective action agreed as per committed time period, CB Secretariat shall prepare a status report and submit it along with the audit report to the certification committee along with recommendations for further decision on suspension or reduction or withdrawal of certification. Critical/major non-conformity may lead to suspension/withdrawal of certification depending on the seriousness.

6.8.4. The surveillance audit reports shall be reviewed and presented to the certification committee in case of any suspension (partial full) of certification or scope extension or scope reduction of the certified CSEs.

6.8.5. The frequency of surveillance audits may be increased based on the type and nature of non-conformities observed, complaints received, market feedback etc. The certified CSEs shall be informed of the reasons for any change in the frequency.

### 6.8.6. Recertification

a. Normally six months prior to completion of the certification term, the certified CSEs shall be informed about the recertification process. The certified CSEs shall apply along with required documents at least 5 months in advance of the expiry date and ensure that audit is carried out normally 3 months before the expiry date. In case the certification process is not completed before the expiry date of certification, the recertification is liable to be withheld till the recertification process is completed.

b. For the purpose of recertification, the re-audit shall be carried out in accordance with process as applied to initial certification process and audit.

c. On completion of the recertification process, the certified CSEs shall initiate the relevant activities to take corrective actions on the observed non-conformities and concerns, if any, and complete all actions as per the criteria of the CB to close all critical & major non-conformities and ensure that corrective action plan for minor non-0conformities are accepted by the audit teams, before the recertification decision can be taken.

d. The audit team shall prepare a report of all the aspects of the audit. As a general policy, certification body ensures that different auditors are deputed in subsequent audits. The final audit report shall be made which clearly identifies the activities undertaken as part of re-audit process.

e. The report shall be prepared as per the laid down guidelines and criteria by the team leader / team members in the established formats listing the level of compliance to the requirement of the certification criteria of the CB. The reports of the re-audit, and the corrective actions taken by the certified CSEs along with recommendations of CB shall then be presented to the certification committee for a decision.

f. If the decision by the certification committee is to continue the certification, a fresh set of certification documents shall be issued to the certified CSEs.

g. All re-audit activities shall be completed prior to the expiry of certification. In case there is a delay in decision-making, the certification shall continue, if the report of the audit team is satisfactory. The decision of the certification committee shall be binding on the certified CSEs.

h. If the certification committee is not able to take a positive decision for any reason, the recertification may be withheld and communicated to the certified CSEs for initiating the appropriate actions including any corrective actions. The certified CSEs shall complete all actions within 6 months failing which the recertification may not be agreed to. The period from the date of previous expiry to recertification shall be deemed to be suspension and recertification effected from the original date of expiry.

## 6.9 Suspension and Withdrawal of Certification

Certification Committee is authorized to decide about the suspension or withdrawal of certification or revoking of suspension.

6.9.1. **Suspension of Certification (Partial / full)**

a. In addition to the requirements specified for Suspension of Certification (Partial or full) the following shall further apply. The certified CSEs may seek on its own suspension of certification citing reasons for the same with justification.

b. The period of suspension will not exceed six months. If the certified CSEs does not take suitable corrective action to the satisfaction of the CB and its audit team within six months, the CB reserves the right to withdraw the certification.

c. In the event of part or complete suspension, with regards to scopes under certification or the certification Scheme, the certified CSEs shall be informed.

d. For revoking suspension, the certified CSEs shall formally apply to CB as per the established guidelines. The suspension shall be revoked after an audit has been carried out to verify that the corrective actions have been implemented and are effective in eliminating the reasons of suspension.

6.9.2. **Withdrawal of Certification**

a. Reasons for withdrawal of certification are given in clause 6.4.4 of this section. Additionally, the CB may decide to withdraw certification based on market feedback, complaints about the CSMS etc. after due investigation and providing the certified CSEs with an opportunity to respond to the findings.

b. In the event of the decision to withdraw the certification, the certified CSEs shall be asked to return the original of certificate and the enclosure of scopes to the CB and to stop using the certification symbol. The CB shall also notify the legal course for initiating any penalty of such misuses if it is reported and found supported by facts and evidence.

c. In case a certified CSEs is found using CB certification symbol after withdrawal of certification supported by facts and evidence, CB may initiate legal action.

d. The following withdrawal of certification, the certified CSEs may seek fresh certification as a new applicant only after a cooling period of minimum one year. CB shall have the right to satisfy itself if the reasons which led to withdrawal have been addressed adequately before accepting the application. Any visits needed for such a check would be charged to the certified CSEs.

6.9.3. **Public Information of Suspension or Withdrawal of Certification**

The information about suspension or withdrawal shall be placed on the CB website in the register of the certified organizations and CB may make a public declaration in the newspapers. The charges for making the information public through newspapers shall be recovered from the certified CSEs involved before revoking the suspension or renewal of the certification.

6.10 **Change in the status of the CSEs**

6.10.1. As part of the application for certification, the applicant / certified CSEs undertakes to inform CB within 30 days if any change takes place in any of the aspects of its status or operation that affects its:

a. Legal, commercial or organisational status
b. The organisation, top management and key personnel
c. Significant changes in Policies and/or documented processes.
d. Premises
e. Personnel, equipment, facilities, working environment or other resources, where significant and relevant.
f. Capability of CSMS or scope of certified activities, or conformity with the requirements of the certification criteria.
g. Addition/closure of any branches / foreign locations where clients are located / operations related to scope.
h. Other such matters that may affect the ability of the CSEs to fulfil requirements for certification.

6.10.2. On receipt of the information of change in any of the above parameters, the CB decides whether an extraordinary visit is necessary, or the change shall not affect the operation of the CSMS within the certified scope. If the CB decides on a visit, such a visit shall be charged as per prevailing fee structure. The invoice for such surveillance visit is sent to the CSEs. Further action shall be initiated only on timely payment of fee for the surveillance visit.

6.10.3. During regular surveillance, the certified CSEs is asked to confirm that no change in the parameters mentioned above or any other aspect that will affect the certification has taken place since the last audit.

6.10.4. In case a certified CSEs is found to have given a wilful wrong declaration, the CB shall initiate suitable action and also shall reserves the right to suspend / withdraw the certification.

### 6.11 Extension / Reduction of the Scope

6.11.1. The extension of scope may be within the same certification standard for new field/subgroup/technical area as applicable.

6.11.2. Normally the extension of the scope will be carried out as part of the surveillance visit by increasing the number of Auditor man-days necessary, or alternatively CB or the CSEs may ask for an additional audit. In case of extension of scope under the same certification standard, the decision of extending the scope may be done based on the audit.

6.11.3. The proposal for the application and other fees for extension of the scope shall be forwarded to the CSEs.

6.11.4. The scope extension visits shall be charged as per the prevailing fee structure. Further action shall be initiated only after timely payment of fee for the scope extension visit. The process followed for the audit and decision for extension of the scope is similar to the initial audit as described in in this document.

6.11.5. The reduction of the scopes is decided based on the following:

a. The certified CSEs may like to reduce their scope of certification of their own accord.

b. The certified CSEs has been placed under partial suspension on account of inadequate resources for part of the scopes and subsequently agrees for the reduction of scope.

### 6.12 Fee payable for the certification, process and Annual Fee

The CB shall abide by the commercials as applicable.

### 6.13 Complaints and Appeals

#### 6.13.1. Complaints

a. Complaint can be made by any person/ consumer or body against the following:

i. The CB, its operation and/ or process
ii. The Auditors, experts, committee members or staff of the CB
iii. Audit process followed by the Auditors and/or by the CB
iv. Misuse of the certified status either in scope or in use of the certification body mark or symbol
v. Quality of CSMS of certified organisation
vi. Clients of CSEs

b. The complaint shall be made in writing (by any means such as letter/ email etc.) to the CB with complete details of the complainant (name, address, organisation etc.) and description of the complaint with supporting information / documents as relevant and necessary.

c. Any complaint received is reviewed to establish if it is related to CB certification (certificates issued with by CB or CSEs' practices relating to CB certification). If so, the CB validates the complaint based on verification of all necessary information gathered and then the complaint is registered and the CB process for handling complaints is followed.

d. The CB will arrange to acknowledge the complaint within one week (excluding postal time, if any). In case any more information / document is needed, the same shall be sought from the complainant/ any other party as decided by the Board. If the complaint does not fall under the domain of CB, the complainant shall be informed of the same while providing possible assistance like referring the complaint to concerned certification body.

e. If the complaint has no details of the complainant or the description is not adequate, the CB will reserve the right of dealing with the complaint as deemed fit.

f. In case the complaint pertains to other certifications but relates to CB certified CSEs, then the concerned certification body is informed, and efforts are also made to seek information from the certified CSEs. Based on any inputs received

from the certified CSEs, the complainant is advised to follow up with the CB. CB also pursues with the other CB.

g. If the complaint is against the non-compliance of certification criteria by any applicant or certified CSEs, then CB shall encourage the complainant to utilize the complaint handling process of the relevant CSEs. At the same time, CB shall also gather all necessary information for establishing validity of the complaint. If the complainant insists and the CSEs agrees, then CB may carry out the investigation. The report of the analysis or parts there of as deemed necessary may be shared with the complainant and the CSEs along with the invoice as applicable to recover the cost of such complaint analysis.

h. In case the complaint pertains to a certified CSEs, the complaint would be referred to the certified CSEs for possible resolution. If the complainant is not satisfied with the response of the certified CSEs, the complaint would be taken up further.

i. In case a complaint is received through some other organisation/stakeholder, and not directly from the complainant, then the organization would be briefed of the outcome at the end of the process.

j. The decision to be communicated to the complainant will be made/reviewed and approved by individuals not involved in the activities in question.

k. The CB will follow each complaint to conclusion and initiate appropriate corrective actions, in case the handling of complaints indicates some issues with CB process. Effectiveness of such actions would be assessed and reported in the Management review meetings. In respect of complaint against a CB applicant / certified CSEs, if established, the CB shall take appropriate actions as deemed fit which may even result in penal actions such as rejection of application or suspension/withdrawal of certification etc.

l. CB will make all efforts to process / resolve the complaint within 1 month, unless it requires more time depending on the nature of the complaint. The CB will provide periodic updates on the progress of complaint investigation as well as information about its outcome to the complainant.

m. The CB will give a formal notice at the end of the complaint handling process to the complainant.

n. The CB will ensure that investigation and decision on complaints do not result in any discriminatory actions.

6.13.2. **Appeals**

a. Any CB applicant/certified CSEs can file an appeal against the decision of the CB to the SO and SM. SO will forward the same to SM. SM may call for details of information/ATR from CB and provide directions. SM shall submit the executive summary of the same to the SO.

b. The appeal shall be filed in writing within thirty days of the decision of the CB along with all the necessary information / documents in support of the appeal.

c. The CB shall have a process of its own to handle all complaints and appeal with clearly defined roles and responsibilities and timelines.

6.13.3. **Records**

CB would maintain a record of all complaints and appeals received, actions taken, corrective actions, if any, and their effectiveness. These records would be maintained for a period of 5 years.

6.13.4. **Publishing of the Information for Public & Availability of Certification Schemes**

a. The CB shall make public announcement of the certification Schemes, criteria of certification, application for certification, fee schedule and other related documents on its website and on specific request.

b. The CB shall maintain a list of the certified CSEs and the applicants on its website. It also makes this information available on request.

c. The certification Schemes are open to all applicants within the capability and scope of the CB.

d. The CB shall also make public information about suspension withdrawal of certification, with holding of recertification and extension of validity of certification.

6.14 **Confidentiality and Disclosure**

The information obtained regarding the CSMS of the applicant and certified CSEs that are not of the nature of public information, shall be kept confidential by all the personnel, members of the CB, panel of Auditors, experts and the committee members.

If the CB has to share any confidential information due to any legal situation, the concerned CSEs shall be informed of the extent of disclosure and the body to whom the disclosure has been made.

6.15 **Use of Scheme Mark**

6.15.1 The Scheme mark is associated with the organisations who have been certified by CB as per the applicable requirements and criteria.

6.15.2 The Scheme mark can only be used under the authority of the certification body. Any unauthorised or misuse of the mark shall lead to suspension/withdrawal of certification and initiation of action as deemed necessary by the certification body.

6.15.3 Certification body at the time of the certification, will inform the client about the use of Scheme mark/mark for display and publicity.

6.15.4 The certified client shall submit to the certification body the form in which he proposes to use the certificate of registration and Scheme mark.

6.15.5 The certified client shall not use the Scheme mark, which mislead the information.

6.15.6 Upon suspension or withdrawal/cancellation of certificate of registration the Scheme mark/ marks in all the products/publicity material to be withdrawn immediately.

6.16 **Termination**

6.16.1 If certification is withdrawn from the certified organisation in full, the organisation shall immediately cease use and distribution of any certificates, stationery and literature bearing the Scheme mark.

6.16.2 If certification is withdrawn from a certified organisation in respect of some of its activities, the organisation shall immediately cease the use and distribution of any stationery and literature bearing the Scheme mark.

6.16.3 The general conditions regarding the use of Scheme mark are given below:

a. The CSMS Scheme mark shall always appear as indicated on the certificate.
b. The minimum size of the mark for display is not specified. However, it shall not be displayed in a size which becomes unidentifiable or unreadable to the unaided eye. Aspect ratio will always be 1:1.
c. Colour combination will not be changed. No alteration shall be carried out in the image. The mark has to be used in full whenever used.
d. Certification body encourages the use of CSMS Scheme mark, by certified organisation in their publicity and promotion. Use of the mark shall be restricted to correspondence, advertisement and promotion relating to the certified CSE.
e. The certified organization shall identify the scope of certification to which the certificate applies when using the mark in any context where the scope of certification is open to doubt.
f. The mark shall not be displayed on or in association with product or packaging which contains a product, process or service supplied by the certified CSE.
g. It is not permitted to use CSMS Scheme mark to be applied by certified clients to laboratory test, calibration or inspection reports or certificates.

Note: It is obligatory on the part of certified organisation to seek the prior approval of certification body regarding the form in which it proposes to use the CSMS mark. The mark shall not be displayed in promotion or advertising by any organisation other than that stated on the certificate.

6.16.4 Use of Scheme mark (Accreditation body's mark) - As specified by Accreditation body.

6.16.5 All CSMS certified CSEs are permitted to use Scheme mark as per the ‘Section 7: Rules for Use of Scheme Mark’.

**Annexure A**

## Audit Duration

The Following components required to define the audit duration which shall be as follows for the minimum requirements.

i. Audit stage 1 - Document review (Manuals, process, other documents as needed – minimum 3-man days for initial certification, 2 man days for recertification and 1 man day for each subsequent certifications Schemes for both initial and recertification.

ii. Review of corrective actions and revised documents – to be estimated by CB Secretariat

iii. Audit stage 2 - Onsite audit – Minimum 4 man-days, to calculate that no. of man-days based on plant size, complexity and variety of control systems, security capability of the control system and application of compensating countermeasures. Lead Assessor in consultation with CSE representative shall finalise and document the same.

iv. Branch office / sub-contractor audit – minimum 1 man day depending on the activities carried out in the branch.

v. Follow up audits – To be estimated by CB.

vi. In case of initial certification audit, the preparation of final report by team leader and/or virtual closing meeting - 1.5 man-day

vii. Review of response to NCs - as per document on timelines for audit process

viii. Surveillance audits – for calculation of man-days refer to note below.

Any extension of scope audit – To be estimated by CB. May require onsite audit.

**Note:** The CB shall have a procedure for efforts estimation in terms of audit man-days including technical expert for ATC (Level 3) audit.

**Section 5**

# REQUIREMENTS FOR CERTIFICATION BODIES

## 1. Scope

This document specifies the requirements for a third-party certification body to undertake certification of Critical Sector Entities for attesting compliance as per the requirements of the CSMS for ATC (Level 3).

## 2. Requirements

2.1. The Certification Bodies operating Cyber Security Management Systems Certification shall comply with the requirements specified in **IS/ISO/IEC 27006:2015 Amendment 1, 2020** - "**Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems" and Additional, Refined, as defined in this document.**

2.2. The main body of this document is generic in nature. The requirements which are normative in nature are defined in annex A of this Section. There are common requirements between this document and the **'Certification Process'**. This document shall be read in conjunction with 'Section 4: Certification Process' of this document.

## 3. Structure of the document

3.1. This document is the adaptation of IS/ISO/IEC 27006:2015 Amendment 1, 2020 'Information technology' which is based on IS/ISO/IEC 17021-1.

3.2. The major functional areas governed are general requirements pertaining to general requirements pertaining to legal, impartiality, liability and financing etc. and core requirements such as CB organisation, resources, information, process and management systems.

3.3. The reference for CB to audit CSE is ATC (Level 3) (refer to Section 3 of this document).

3.4. The human resource specifically the auditors of CB shall have adequate knowledge of the 'Additional Technical Criteria (Level 3)' and the accompanying 'Certification Process'.

## 4. Duration of audits undertaken by the Certification Body

The calculation of audit man day shall be guided as per annex A of 'Section 4: Certification Process'.

4.1. The CB shall have procedures to determine the audit man days required for audit for initial assessment, surveillance, and reassessment. The procedure shall also include the policies for estimation of audit duration for multisite organizations and transfer of certificates, as needed.

## 5. Requirements for Approval

5.1. The CBs are required to demonstrate that they have an experience of auditing minimum 2 clients (CSEs) as per this STC (Level 2) so that AB has sufficient data to analyse that CBs have processes and capabilities in place to perform the audit/certification of CSEs effectively.

5.2. The requirements for approval of a CB are based on IS/ISO/IEC 17021-1:2015 and IS/ISO/IEC 27006: 2015 (with Amendments) which is referred at Annex A of this section. This shall be used for the following purposes:

5.2.1. For CBs to demonstrating compliance and obtaining approval. The Annex A of this section will facilitate CBs to prepare Document Review Report (DRR).

5.2.2. By AB as an assessment checklist for conducting the audit.

5.3. Since at this stage, the CBs are already accredited to operate CSMS certification of BTC (Level 1) and STC (Level 2), the AB shall verify the compliance with the requirements to ATC (Level 3) which are labelled as 'CS-L3', wherever applicable, in annex A of this section. The contents of IS/ISO/IEC 17021-1:2015 are retained in annex A of this section to establish the context with ICS and maintain homogeneity with ATC (Level 3).

## Annexure A

## Requirement for Certification Bodies operating CSMS Scheme for Additional Technical Criteria (Level 3)

The requirements are adopted from IS/ISO/IEC 17021-1:2015 and IS/ISO/IEC 27006:2015 Amendment, 2022. These are amended/enhanced to be compatible with the requirements of CSMS for ATC (Level 3) and are prefixed with CS-L3. All other requirements of IS are applicable.

Note 1: CSMS in this Annex A implies CSMS for ATC (Level 3). The concept of ISMS extends to CSMS for ATC (Level 3) and not and the same is not amended.

Note 2: Annexures mentioned in IS clauses refer to the IS/ISO/IEC 27006:2015 Amendment, 2022.

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| **5** | **General Requirement** |
| **5.1** | **Legal and contractual matters** |
| 5.1.1 | **Legal responsibility** |
| | Certification body shall be a legal entity, or a defined part of a legal entity, such that it can be held legally responsible for all its certification activities. A governmental certification body is deemed to be a legal entity on the basis of its governmental status. |
| CS-L3 | The CB shall have obtained accreditation for BTC (Level 1) and STC (Level 2). |
| 5.1.2 | **Certification agreement** |
| | The certification body shall have a legally enforceable agreement with each client for the provision of certification activities in accordance with the relevant requirements of this part of IS/ISO/IEC 17021. In addition, where there are multiple offices of a certification body or multiple sites of a client, the certification body shall ensure there is a legally enforceable agreement between the certification body granting certification and the client that covers all the sites within the scope of the certification. |
| | **Note** An agreement can be achieved through multiple agreements that reference or otherwise link to one another. |
| CS-L3 | The agreement shall cover vertical & horizontal interdependencies between organisation layers & in-bound & out-bound interdependencies. |
| 5.1.3 | Responsibility for certification decisions |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | The certification body shall be responsible for, and shall retain authority for, its decisions relating to certification, including the granting, refusing, maintaining of certification, expanding or reducing the scope of certification, renewing, suspending or restoring following suspension, or withdrawing of certification. |
| **5.2** | **Management of impartiality** |
| 5.2.1 | Conformity assessment activities shall be undertaken impartially. The certification body shall be responsible for the impartiality of its conformity assessment activities and shall not allow commercial, financial or other pressures to compromise impartiality. |
| *IS 5.2.1* | IS 5.2 Conflicts of interest |
| | Certification bodies may carry out the following duties without them being considered as consultancy or having a potential conflict of interest: |
| | Arranging and participating as a lecturer in training courses, provided that, where these courses relate to information security management, related management systems or auditing, certification bodies shall confine themselves to the provision of generic information and advice which is publicly available, i.e. they shall not provide company-specific advice which contravenes the requirements of b) below; |
| | Making available or publishing on request information describing the certification body's interpretation of the requirements of the certification audit standards (see 9.1.3.6); |
| | Activities prior to audit, solely aimed at determining readiness for certification audit; however, such activities shall not result in the provision of recommendations or advice that would contravene this clause and the certification body shall be able to confirm that such activities do not contravene these requirements and that they are not used to justify a reduction in the eventual certification audit duration; |
| | Performing second and third-party audits according to standards or regulations other than those being part of the scope of accreditation; |
| | Adding value during certification audits and surveillance visits, e.g. by identifying opportunities for improvement, as they become evident during the audit, without recommending specific solutions. |
| | The certification body shall not provide internal information security reviews of the client's ISMS subject to certification. Furthermore, the certification body shall be independent from the body or bodies (including any individuals) which provide the internal ISMS audit. |
| CS-L3 | The certification body shall not conduct internal cyber security reviews of the CSEs, CSMS BTC (Level 1), STC (Level 2) and ATC (Level 3). Furthermore, the certification |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | body shall be independent from the body or bodies (including any individuals) which provide the internal CSMS audit. |
| CS-L3 | TBs providing organisation specific trainings and their trainers performing assessment is a conflict of interest. The empanelled freelance trainers and consultant shall be dealt through a process ensuring that there are no conflict of interest for a particular client/CSE. |
| 5.2.2 | The certification body shall have top management commitment to impartiality in management system certification activities. The certification body shall have a policy that it understands the importance of impartiality in carrying out its management system certification activities, manages conflict of interest and ensures the objectivity of its management system certification activities. |
| 5.2.3 | The certification body shall have a process to identify, analyse, evaluate, treat, monitor, and document the risks related to conflict of interests arising from provision of certification including any conflicts arising from its relationships on an ongoing basis. Where there are any threats to impartiality, the certification body 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 certification body or from the activities of other persons, bodies or organizations. When a relationship poses an unacceptable threat to impartiality (such as a wholly owned subsidiary of the certification body requesting certification from its parent), then certification shall not be provided. |
| | Top management shall review any residual risk to determine if it is within the level of acceptable risk. |
| | The risk assessment process shall include identification of and consultation with appropriate interested parties to advise on matters affecting impartiality including openness and public perception. The consultation with appropriate interested parties shall be balanced with no single interest predominating. |
| | **Note 1** Sources of threats to impartiality of the certification body 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** Interested parties can include personnel and clients of the certification body, customers of organizations whose management systems are certified, representatives of industry trade associations, representatives of governmental regulatory bodies or other governmental services, or representatives of non-governmental organizations, including consumer organizations. |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | **Note 3** One way of fulfilling the consultation requirement of this clause is by the use of a committee of these interested parties. |
| CS-L3 | **Note** 4: ICS OEMs, System Integrator and Service Provider are interested parties and have a significant role for capability demonstration and security levels compliance as per ATC (Level 3). |
| 5.2.4 | A certification body shall not certify another certification body for its management system certification activities |
| 5.2.5 | The certification body and any part of the same legal entity and any entity under the organisational control of the certification body [see 9.5.1.2, bullet b)] shall not offer or provide management system consultancy. This also applies to that part of government identified as the certification body. |
| | **Note** This does not preclude the possibility of exchange of information (e.g. explanation of findings or clarification of requirements) between the certification body and its clients. |
| 5.2.6 | The carrying out of internal audits by the certification body and any part of the same legal entity to its certified clients is a significant threat to impartiality. Therefore, the certification body and any part of the same legal entity and any entity under the organizational control of the certification body [see 9.5.1.2, bullet b)] shall not offer or provide internal audits to its certified clients. A recognized mitigation of this threat is that the certification body shall not certify a management system on which it provided internal audits for a minimum of two years following the completion of the internal audits. |
| | **Note** See Note 1 to 5.2.3. |
| 5.2.7 | Where a client has received management systems consultancy from a body that has a relationship with a certification body, this is a significant threat to impartiality. A recognized mitigation of this threat is that the certification body shall not certify the management system for a minimum of two years following the end of the consultancy. |
| | **Note** See Note 1 to 5.2.3. |
| 5.2.8 | The certification body shall not outsource audits to a management system consultancy organisation, as this poses an unacceptable threat to the impartiality of the certification body (see 7.5). This does not apply to individuals contracted as auditors covered in 7.3. |
| 5.2.9 | The certification body's activities shall not be marketed or offered as linked with the activities of an organization that provides management system consultancy. The certification body shall take action to correct inappropriate links or statements by any consultancy organization stating or implying that certification would be simpler, easier, faster or less expensive if the certification body were used. A certification body shall not |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | state or imply that certification would be simpler, easier, faster or less expensive if a specified consultancy organization were used. |
| 5.2.10 | In order to ensure that there is no conflict of interests, personnel who have provided management system consultancy, including those acting in a managerial capacity, shall not be used by the certification body to take part in an audit or other certification activities if they have been involved in management system consultancy towards the client. A recognized mitigation of this threat is that personnel shall not be used for a minimum of two years following the end of the consultancy. |
| 5.2.11 | The certification body shall take action to respond to any threats to its impartiality arising from the actions of other persons, bodies or organizations. |
| 5.2.12 | All certification body personnel, either internal or external, or committees, who could influence the certification activities, shall act impartially and shall not allow commercial, financial or other pressures to compromise impartiality. |
| 5.2.13 | Certification bodies shall require personnel, internal and external, to reveal any situation known to them that can present them or the certification body with a conflict of interests. Certification bodies shall record and use this information as input to be identifying threats to impartiality raised by the activities of such personnel or by the organizations that employ them, and shall not use such personnel, internal or external, unless they can demonstrate that there is no conflict of interest. |
| **5.3** | **Liability and financing** |
| 5.3.1 | The certification body shall 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. |
| 5.3.2 | The certification body shall evaluate its finances and sources of income and demonstrate that initially, and on an ongoing basis, commercial, financial or other pressures do not compromise its impartiality. |
| **6** | **Structural requirements** |
| **6.1** | **Organisational structure and top management** |
| 6.1.1 | The certification body shall document its organizational structure, duties, responsibilities and authorities of management and other personnel involved in certification and any committees. When the certification body is a defined part of a legal entity, the structure shall include the line of authority and the relationship to other parts within the same legal entity. |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| 6.1.2 | Certification activities shall be structured and managed so as to safeguard impartiality. |
| 6.1.3 | The certification body shall identify the top management (board, group of persons, or person) having overall authority and responsibility for each of the following: |
| | a) Development of policies and establishment of processes and procedures relating to its operations; |
| | b) Supervision of the implementation of the policies, processes and procedures; |
| | c) Ensuring impartiality; |
| | d) Supervision of its finances; |
| | e) Development of management system certification services and schemes; |
| | f) Performance of audits and certification, and responsiveness to complaints; |
| | g) Decisions on certification; |
| | h) Delegation of authority to committees or individuals, as required, to undertake defined activities on its behalf; |
| | i) Contractual arrangements; |
| | j) Provision of adequate resources for certification activities. |
| 6.1.4 | The certification body shall have formal rules for the appointment, terms of reference and operation of any committees that are involved in the certification activities. |
| **6.2** | **Operational control** |
| 6.2.1 | The certification body shall have a process for the effective control of certification activities delivered by branch offices, partnerships, agents, franchisees, etc., irrespective of their legal status, relationship or geographical location. The certification body shall consider the risk that these activities pose to the competence, consistency and impartiality of the certification body. |
| 6.2.2 | The certification body shall consider the appropriate level and method of control of activities undertaken including its processes, technical areas of certification bodies' operations, competence of personnel, lines of management control, reporting and remote access to operations including records. |
| **7** | **Resource requirements** |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| **7.1** | **Competence of personnel** |
| 7.1.1 | **General considerations** |
| | The certification body shall have processes to ensure that personnel have appropriate knowledge and skills relevant to the types of management systems (e.g. environmental management systems, quality management systems, information security management systems) and geographic areas in which it operates. |
| CS-L3 | The certification body shall have processes to ensure that personnel have appropriate knowledge and skills relevant to ATC (Level 3). This includes cyber security issues in ICS, IEC 62443 family of standards and requirements of ATC (Level 3). For details, refer to Annex B of this section. |
| CS-L3 | The personnel involved in certification activities such as Auditors, lead Audits, CB secretariat, Technical Experts shall have undergone the process of police verification and background check and records shall be maintained. |
| IS 7.1.1 | **General considerations** |
| IS 7.1.1.1 | **Generic competence requirements** |
| | The certification body shall ensure that it has knowledge of the technological, legal and regulatory developments relevant to the ISMS of the client which it assesses. |
| | The certification body shall define the competence requirements for each certification function as referenced in Table A.1 of IS/ISO/IEC 17021-1. The certification body shall take into account all the requirements specified in IS/ISO/IEC 17021-1 and 7.1.2 and 7.2.1 of this International Standard that are relevant for the ISMS technical areas as determined by the certification body. |
| | **Note** Annex A of ISO 27006 provides a summary of the competence requirements for personnel involved in specific certification functions. |
| CS-L3 | The certification body shall ensure that it has knowledge of the technological, legal and regulatory developments relevant to the CSMS ATC (Level 3) which it assesses. The certification body shall define the competence requirements for CSMS ATC (Level 3) for certification functions as per Annex B of this Section . This CB shall have process to extend the scope of assessment of CSMS BTC (Level 1) and STC (Level 2) to ATC (Level 3). The certification body shall define the competence requirements for their ATC (Level 3) certification programme ensuring technical areas *industrial control systems* specific requirements are addressed. |
| CS-L3 | CB shall have a robust continuous process to assess the competence (knowledge and skill) of all the personnel involved in the activities of conformity assessment so that the |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | rigour of the process is maintained at all times. AB shall exercise oversight over the CB specifically on the criteria for selection and onboarding of personnel (conducting applicable knowledge and skill tests for all the personnel involved in certification related activities) executing certification as per the laid down criteria. |
| 7.1.2 | **Determination of competence criteria** |
| | The certification body shall have a process for determining the competence criteria for personnel involved in the management and performance of audits and other certification activities. Competence criteria shall be determined with regard to the requirements of each type of management system standard or specification, for each technical area, and for each function in the certification process. The output of the process shall be the documented criteria of required knowledge and skills necessary to effectively perform audit and certification tasks to be fulfilled to achieve the intended results. Annex A specifies the knowledge and skills that a certification body shall define for specific functions. Where additional specific competence criteria have been established for a specific standard or certification scheme (e.g., IS/ISO/IEC TS 17021-2, IS/ISO/IEC TS 17021-3 or ISO/TS 22003), these shall be applied. |
| CS-L3: | The certification body shall have a process for determining the competence criteria for personnel involved in the management and performance of audits and other certification activities of ATC (Level 3). The output of the process shall be the documented criteria of required knowledge and skills necessary to effectively perform audit and certification tasks to be fulfilled to achieve the intended results. Annex B of this Section specifies the knowledge and skills that a certification body shall define for specific functions. |
| | **Note** The term “technical area” is applied differently depending on the management system standard being considered. For any management system, the term is related to products, processes and services in the context of the scope of the management system standard. The technical area can be defined by a specific certification scheme (e.g. ISO/TS 22003) or can be determined by the certification body. It is used to cover a number of other terms such as “scopes”, “categories”, “sectors”, etc., which are traditionally used in different management system disciplines. |
| IS 7.1.2 | **IS 7.1.2 Determination of Competence Criteria** |
| IS 7.1.2.1 | **Competence requirements for ISMS auditing** |
| IS 7.1.2.1.1 | **General requirements** |
| | The certification body shall have criteria for verifying the background experience, specific training or briefing of audit team members that ensures at least: |
| | a) Knowledge of information security; |
| | b) Technical knowledge of the activity to be audited; |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | c) Knowledge of management systems; |
| | d) Knowledge of the principles of auditing; |
| | **Note** Further information on the principles of auditing can be found in ISO 19011. |
| | e) Knowledge of ISMS monitoring, measurement, analysis and evaluation. |
| | These above requirements a) to e) apply to all auditors being part of the audit team, with exception of b), which can be shared among auditors being part of the audit team. |
| | The audit team shall be competent to trace indications of information security incidents in the client's ISMS back to the appropriate elements of the ISMS. |
| | The audit team shall have appropriate work experience of the items above and practical application of these items (this does not mean that an auditor needs a complete range of experience of all areas of information security, but the audit team as a whole shall have enough appreciation and experience to cover the ISMS scope being audited). |
| CS-L3 | The certification body shall have criteria for verifying the background experience, specific training or briefing of audit team members that ensures at least: |
| | a) Knowledge of cyber security; |
| | b) Knowledge of CSMS (Level 1, 2 and 3) monitoring, measurement, analysis and evaluation. |
| | The audit team shall be competent to trace indications of information security incidents in the client's CSMS back to the appropriate elements of the CSMS. |
| | The audit team shall have appropriate work experience of the items above and practical application of these items (this does not mean that an auditor needs a complete range of experience of all areas of information security, but the audit team as a whole shall have enough appreciation and experience to cover the CSMS scope being audited). |
| IS 7.1.2.1.2 | **Information security management terminology, principles, practices and techniques** |
| | Collectively, all members of the audit team shall have knowledge of: |
| | a) ISMS specific documentation structures, hierarchy and interrelationships; |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | b) Information security management related tools, methods, techniques and their application; |
| | c) Information security risk assessment and risk management; |
| | d) Processes applicable to ISMS; |
| | e) The current technology where information security may be relevant or an issue. |
| | Every auditor shall fulfil a), c) and d). |
| CS-L3 | **Cyber security management terminology, principles, practices and techniques** |
| | Collectively, all members of the audit team shall have knowledge of: |
| | a) CSMS specific documentation structures, hierarchy and interrelationships; |
| | b) Cyber security management related tools, methods, techniques and their application; |
| | c) Cyber security risk assessment and risk management; |
| | d) Processes applicable to CSMS; |
| | e) The current technology where cyber security may be relevant or an issue. |
| | Every auditor shall fulfil a), c) and d). |
| IS 7.1.2.1.3 | **Information security management system standards and normative documents** |
| | Auditors involved in ISMS auditing shall have knowledge of: |
| | a) All requirements addressed in IS/ISO/IEC 27001. |
| | Collectively, all members of the audit team shall have knowledge of: |
| | b) All controls addressed in IS/ISO/IEC 27002 (if determined as necessary also from sector specific standards) and their implementation, categorized as: |
| | 1) Information security policies; |
| | 2) Organisation of information security; |
| | 3) Human resource security; |
| | 4) Asset management; |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | 5) Access control, including authorization; |
| | 6) Cryptography; |
| | 7) Physical and environmental security; |
| | 8) Operations security, including IT-services; |
| | 9) Communications security, including network security management and information transfer; |
| | 10) System acquisition, development and maintenance; |
| | 11) Supplier relationships, including outsourced services; |
| | 12) Information security incident management; |
| | 13) Information security aspects of business continuity management, including redundancies; |
| | 14) Compliance, including information security reviews |
| CS-L3 | **Cyber security management system standards and normative documents** |
| | Auditors involved in CSMS auditing shall have knowledge of: |
| | a) foundational requirements and all the requirements addressed in ATC (Level 3) |
| | Collectively, all members of the audit team shall have knowledge of: |
| | b) All controls addressed in ATC (Level 3) (if determined as necessary also from sector specific standards) and their implementation, categorized as: |
| | 1) Cyber security policies; |
| | 2) Organisation of cyber security; |
| | 3) Cyber security incident management; |
| | 4) Cyber security aspects of business continuity management, including redundancies; |
| | 5) compliance, including cyber security reviews |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| CS-L3 | Certification body personnel responsible for certification management (also known as certification officer) shall undergo training on ICS Cyber Security (Foundation) (ICS-F) |
| IS 7.1.2.1.4 | **Business management practices** |
| | Auditors involved in ISMS auditing shall have knowledge of: |
| | a) Industry information security good practices and information security procedures; |
| | b) Policies and business requirements for information security; |
| | c) General business management concepts, practices and the inter-relationship between policy, objectives and results; |
| | d) Management processes and related terminology. |
| | **Note** These processes also include human resources management, internal and external communication and other relevant support processes |
| CS-L3 | **Business management practices** |
| | Auditors involved in CSMS auditing shall have knowledge of: |
| | a) Industry information security good practices and cyber security procedures; |
| | b) Policies and business requirements for cyber security; |
| IS 7.1.2.1.5 | **Client business sector** |
| | Auditors involved in ISMS auditing shall have knowledge of: |
| | a) The legal and regulatory requirements in the particular information security field, geography and jurisdiction(s); |
| | NOTE Knowledge of legal and regulatory requirements does not imply a profound legal background. |
| | b) Information security risks related to business sector; |
| | c) Generic terminology, processes and technologies related to the client business sector; |
| | d) The relevant business sector practices. |
| | The criteria a) may be shared amongst the audit team |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| CS-L3 | **Client business sector** |
| | Auditors involved in CSMS auditing shall have knowledge of: |
| | a) The legal and regulatory requirements in the particular cyber security field, geography and jurisdiction(s); |
| | b) Cyber security risks related to business sector; |
| IS 7.1.2.1.6 | **Client products, processes and organization** |
| | Collectively, auditors involved in ISMS auditing shall have knowledge of: |
| | a) The impact of organization type, size, governance, structure, functions and relationships on development and implementation of the ISMS and certification activities, including outsourcing; |
| | b) Complex operations in a broad perspective; |
| | c) Legal and regulatory requirements applicable to the product or service |
| CS-L3 | **Client products, processes and organization** |
| | Collectively, auditors involved in CSMS auditing shall have knowledge of: |
| | a) The impact of organization type, size, governance, structure, functions and relationships on development and implementation of the CSMS and certification activities, including outsourcing; |
| IS 7.1.2.2 | **Competence requirements for leading the ISMS audit team** |
| | In addition to the requirements in 7.1.2.1, audit team leaders shall fulfil the following requirements, which shall be demonstrated in audits under guidance and supervision. |
| | a) Knowledge and skills to manage the certification audit process and the audit team; |
| | b) Demonstration of the capability to communicate effectively, both orally and in writing. |
| CS-L3 | **Competence requirements for leading the CSMS audit team as per Annex B of this Section.** |
| IS 7.1.2.3 | **Competence requirements for conducting the application review** |
| IS 7.1.2.3.1 | **Information security management system standards and normative documents** |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | Personnel conducting the application review to determine audit team competence required, to select the audit team members and to determine the audit time shall have knowledge of: |
| | a) Relevant ISMS standards and other normative documents used in the certification process. |
| CS-L3 | **Information security management system standards and normative documents** |
| | Personnel conducting the application review to determine audit team competence required, to select the audit team members and to determine the audit time shall have knowledge of: |
| | a) Relevant CSMS standards and other normative documents used in the certification process. |
| IS 7.1.2.3.2 | Client business sector |
| | Personnel conducting the application review to determine the audit team competence required, to select the audit team members and to determine the audit time shall have knowledge of: |
| | a) Generic terminology, processes, technologies and risks related to the client business sector |
| IS 7.1.2.3.3 | **Client products, processes and organization** |
| | Personnel conducting the application review to determine audit team competence required, to select the audit team members and to determine the audit time shall have knowledge of: |
| | a) Client products, processes, organization types, size, governance, structure, functions and relationships on development and implementation of the ISMS and certification activities, including outsourcing functions |
| CS-L3 | **Client products, processes and organization** |
| | Personnel conducting the application review to determine audit team competence required, to select the audit team members and to determine the audit time shall have knowledge of: |
| | a) Client products, processes, organization types, size, governance, structure, functions and relationships on development and implementation of the CSMS and certification activities, including outsourcing functions |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| IS 7.1.2.4 | **Competence requirements for reviewing audit reports and making certification decisions** |
| IS 7.1.2.4.1 | **General** |
| | The personnel reviewing audit reports and making certification decisions shall have knowledge that enables them to verify the appropriateness of the scope of certification as well as changes to the scope and their impact on the effectiveness of the audit, in particular the continuing validity of the identification of interfaces and dependencies and the associated risks. |
| | Additionally, the personnel reviewing audit reports and making the certification decisions shall have knowledge of: |
| | a) Management systems in general; |
| | b) Audit processes and procedures; |
| | c) Audit principles, practices and techniques |
| IS 7.1.2.4.2 | **Information security management terminology, principles, practices and techniques** |
| | The personnel reviewing audit reports and making the certification decisions shall have knowledge of: |
| | a) The items listed in 7.1.2.1.2 a), c) and d); (specific to CSMS) |
| | b) Legal and regulatory requirements relevant to information security. |
| CS-L3 | **Cyber security management terminology, principles, practices and techniques** |
| | The personnel reviewing audit reports and making the certification decisions shall have knowledge of: |
| | a) The items listed in 7.1.2.1.2 a), c) and d) (specific to CSMS); |
| | b) Legal and regulatory requirements relevant to cyber security. |
| IS 7.1.2.4.3 | **Information security management system standards and normative documents.** |
| | Personnel reviewing audit reports and making certification decisions shall have knowledge of: |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | a) Relevant ISMS standards and other normative documents used in the certification process |
| CS-L3 | **Cyber security management system standards and normative documents.** |
| | Personnel reviewing audit reports and making certification decisions shall have knowledge of: |
| | a) Relevant CSMS standards and other normative documents used in the certification process |
| IS 7.1.2.4.4 | **Client business sector** |
| | Personnel reviewing audit reports and making certification decisions shall have knowledge of: |
| | a) Generic terminology and risks related to the relevant business sector practices. |
| IS 7.1.2.4.5 | **Client products, processes and organization** |
| | Personnel reviewing audit reports and making certification decisions shall have knowledge of: |
| | a) Client products, processes, organization types, size, governance, structure, functions and relationships |
| CS-L3 | Certification body personnel responsible for certification management (also known as certification officer) shall undergo training on ICS Cyber Security (Foundation) (ICS-F). The responsible persons in CB for reviewing the audit report shall be trained on ATC (Level 3) also. The auditors shall meet the criteria as mentioned in annex B of this section. |
| 7.1.3 | **Evaluation processes** |
| | The certification body shall have documented processes for the initial competence evaluation, and on- going monitoring of competence and performance of all personnel involved in the management and performance of audits and other certification activities, applying the determined competence criteria. The certification body shall demonstrate that its evaluation methods are effective. The output from these processes shall be to identify personnel who have demonstrated the level of competence required for the different functions of the audit and certification process. Competence shall be demonstrated prior to the individual taking the responsibility for the performance of their activities within the certification body. |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | **Note** 1: A number of evaluation methods that can be used to evaluate competence are described in annex B. |
| | **Note** 2: Annex C shows an example of a process flow for determining and maintaining competence. |
| ***7.1.4*** | **Other considerations** |
| | The certification body shall have access to the necessary technical expertise for advice on matters directly relating to certification activities for all technical areas, types of management systems and geographic areas in which the certification body operates. Such advice may be provided externally or by certification body personnel. |
| **7.2** | **Personnel involved in the certification activities** |
| 7.2.1 | The certification body shall have sufficient, competent personnel for managing and supporting the type and range of audit programmes and other certification work performed. |
| CS-L3 | These person should be trained as per ICS Foundation requirements. |
| IS 7.2.1 | **IS 7.2 Demonstration of auditor knowledge and experience** |
| | The certification body shall demonstrate that the auditors have knowledge and experience through: |
| | a) Recognized ISMS-specific qualifications; |
| | b) Registration as auditor where applicable; |
| | c) Participation in ISMS training courses and attainment of relevant personal credentials; |
| | d) Up to date professional development records; |
| | e) ISMS audits witnessed by another CSMS auditor |
| CS-L3 | **IS 7.2 Demonstration of auditor knowledge and experience** |
| | The certification body shall demonstrate that the auditors have knowledge and experience through: |
| | a) Recognized CSMS-specific qualifications; |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | c) Participation in CSMS training courses and attainment of relevant personal credentials; |
| | d) CSMS audits witnessed by another SMS auditor |
| | feConduct of Knowledge and Skill test of audit team. |
| IS 7.2.1.1 | **Selecting auditors** |
| | In addition to 7.1.2.1, the criteria for selecting auditors shall ensure that each auditor: |
| | a) Has professional education or training to an equivalent level of university education; |
| | b) Has at least four years full time practical workplace experience in information technology, of which at least two years are in a role or function relating to information security; |
| | c) Has successfully completed at least five days of training, the scope of which covers ISMS audits and audit management; |
| | d) Has gained experience of auditing ISMS prior to acting as an auditor performing ISMS audits. This experience shall be gained by performing as an auditor-in-training monitored by an ISMS evaluator (see IS/ISO/IEC 17021-1:2015, 9.2.2.1.4) in at least one ISMS initial certification audit (stage 1 and stage 2) or re-certification and at least one surveillance audit. This experience shall be gained in at least 10 ISMS on-site audit days and performed in the last 5 years. The participation shall include review of documentation and risk assessment, implementation assessment.<br>and audit reporting |
| | e) This experience shall be gained by performing as an auditor-in-training monitored by an ISMS evaluator (see IS/ISO/IEC 17021-1:2015, 9.2.2.1.4) in at least one ISMS initial certification audit (stage 1 and stage 2) or re-certification and at least one surveillance audit. This experience shall be gained in at least 10 ISMS on-site audit days and performed in the last 5 years. The participation shall include review of documentation and risk assessment, implementation assessment and audit reporting. |
| | f) Has relevant and current experience; |
| | g) Keeps current knowledge and skills in information security and auditing up to date through continual professional development. |
| | h) Has competence in auditing an ISMS in accordance with IS/ISO/IEC 27001. |
| | Technical experts shall comply with criteria a), b) and e) |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| CS-L3 | **Selecting auditors** |
| | a) Refer to Annex B of this section. |
| | b) Has successfully completed at least five days of training, the scope of which covers CSMS audits and audit management; |
| | c) Has gained experience of auditing CSMS prior to acting as an auditor performing CSMS audits. This experience shall be gained by performing as an auditor-in-training monitored by an CSMS evaluator (see IS/ISO/IEC 17021-1:2015, 9.2.2.1.4) in at least one ISMS initial certification audit (stage 1 and stage 2) or re-certification and at least one surveillance audit. This experience shall be gained in at least 10 ISMS on-site audits of various organisations. The participation shall include review of documentation and risk assessment, implementation assessment and audit reporting. |
| | d) This experience shall be gained by performing as an auditor-in-training monitored by an CSMS evaluator (see IS/ISO/IEC 17021-1:2015, 9.2.2.1.4) in at least one CSMS initial certification audit (stage 1 and stage 2) or re-certification and at least one surveillance audit. This experience shall be gained in at least 10 ISMS/CSMS on-site audits of various organisations. The participation shall include review of documentation and risk assessment, implementation assessment and audit reporting. |
| | g) Keeps current knowledge and skills in information security and auditing up to date through continual professional development. |
| | h) Has competence in auditing an CSMS in accordance with ATC (Level 3). |
| CS-L3 | Certification body personnel responsible for certification management (also known as certification officer) shall undergo training on ICS Cyber Security (Foundation) (ICS-F) and auditors shall meet the competency requirements given in Annex B of this Section. |
| IS 7.2.1.2 | **Selecting auditors for leading the team** |
| | In addition to 7.1.2.2 and 7.2.1.1, the criteria for selecting an auditor for leading the team shall ensure that this auditor: |
| | a) Has actively participated in all stages of at least three ISMS audits. The participation shall include initial scoping and planning, review of documentation and risk assessment, implementation assessment and formal audit reporting |
| 7.2.2 | The certification body shall employ, or have access to, a sufficient number of auditors, including audit team leaders, and technical experts to cover all of its activities and to handle the volume of audit work performed. |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| 7.2.3 | The certification body shall make clear to each person concerned their duties, responsibilities and authorities. |
| 7.2.4 | The certification body shall have processes for selecting, training, formally authorizing auditors and for selecting and familiarizing technical experts used in the certification activity. The initial competence evaluation of an auditor shall include the ability to apply required knowledge and skills during audits, as determined by a competent evaluator observing the auditor conducting an audit. |
| | **Note** During the selection and training process described above desired personal behaviour can be considered. These are characteristics that affect an individual's ability to perform specific functions. Therefore, knowledge about the behaviour of individuals enables a certification body to take advantage of their strengths and to minimize the impact of their weaknesses. Desired personal behaviour that is important for personnel involved in certification activities is described in Annex D. |
| 7.2.5 | The certification body shall have a process to achieve and demonstrate effective auditing, including the use of auditors and audit team leaders possessing generic auditing skills and knowledge, as well as skills and knowledge appropriate for auditing in specific technical areas. |
| 7.2.6 | The certification body shall ensure that auditors (and, where needed, technical experts) are knowledgeable of its audit processes, certification requirements and other relevant requirements. The certification body shall give auditors and technical experts access to an up-to-date set of documented procedures giving audit instructions and all relevant information on the certification activities. |
| 7.2.7 | The certification body shall identify training needs and shall offer or provide access to specific training to ensure its auditors, technical experts and other personnel involved in certification activities are competent for the functions they perform. |
| 7.2.8 | The group or individual that takes the decision on granting, refusing, maintaining, renewing, suspending, restoring, or withdrawing certification, or on expanding or reducing the scope of certification, shall understand the applicable standard and certification requirements, and shall have demonstrated competence to evaluate the outcomes of the audit processes including related recommendations of the audit team. |
| 7.2.9 | The certification body shall ensure the satisfactory performance of all personnel involved in the audit and other certification activities. There shall be a documented process for monitoring competence and performance of all persons involved, based on the frequency of their usage and the level of risk linked to their activities. In particular, the certification body shall review and record the competence of its personnel in the light of their performance in order to identify training needs. |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| 7.2.10 | The certification body shall monitor each auditor considering each type of management system to which the auditor is deemed competent. The documented monitoring process for auditors shall include a combination of on-site evaluation, review of audit reports and feedback from clients or from the market. This monitoring shall be designed in such a way as to minimize disturbance to the normal processes of certification, especially from the client's viewpoint. |
| 7.2.11 | The certification body shall periodically evaluate the performance of each auditor on-site.The frequency of on-site evaluations shall be based on need determined from all monitoring information available. |
| **7.3** | **Use of individual external auditors and external technical experts** |
| | The certification body shall require external auditors and external technical experts to have a written agreement by which they commit themselves to comply with applicable policies and implement processes as defined by the certification body. The agreement shall address aspects relating to confidentiality and impartiality and shall require the external auditors and external technical experts to notify the certification body of any existing or prior relationship with any organization they may be assigned to audit. |
| | **Note** Use of an individual or employee of another organization individually contracted to serve as an external auditor or technical expert does not constitute outsourcing. |
| IS 7.3.1 | IS 7.3 Using external auditors or external technical experts as part of the audit team |
| | Technical experts shall work under the supervision of an auditor. The minimum requirements for technical experts are listed in 7.2.1.1 |
| **7.4** | **Personnel records** |
| | The certification body shall maintain up-to-date personnel records, including relevant qualifications, training, experience, affiliations, professional status and competence. This includes management and administrative personnel in addition to those performing certification activities. |
| **7.5** | **Outsourcing** |
| 7.5.1 | The certification body shall have a process in which it describes the conditions under which outsourcing (which is subcontracting to another organization to provide part of the certification activities on behalf of the certification body) may take place. The certification body shall have a legally enforceable agreement covering the arrangements, including confidentiality and conflicts of interests, with each body that provides outsourced services. |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| 7.5.2 | Decisions for granting, refusing, maintaining of certification, expanding or reducing the scope of certification, renewing, suspending or restoring, or withdrawing of certification shall not be outsourced. |
| 7.5.3 | The certification body shall: |
| | a) Take responsibility for all activities outsourced to another body; |
| | b) Ensure that the body that provides outsourced services, and the individuals that it uses, conform to requirements of the certification body and also to the applicable provisions of this part of IS/ISO/IEC 17021, including competence, impartiality and confidentiality; |
| | c) Ensure that the body that provides outsourced services, and the individuals that it uses, are not involved, either directly or through any other employer, with an organization to be audited, in such a way that impartiality could be compromised. |
| 7.5.4 | The certification body shall have a process for the approval and monitoring of all bodies that provide outsourced services used for certification activities, and shall ensure that records of the competence of all personnel involved in certification activities are maintained. |
| | **Note** 1 For 7.5.1 to 7.5.4, where the certification body engages individuals or employees of other organizations to provide additional resources or expertise, these individuals do not constitute outsourcing provided they are individually contracted to operate under the certification body's management system (see 7.3). |
| | **Note** 2 For 7.5.1 to 7.5.4, the terms "outsourcing" and "subcontracting" are considered to be synonyms. |
| **8** | **Information requirements** |
| **8.1** | **Public information** |
| 8.1.1 | The certification body shall maintain (through publications, electronic media or other means), |
| | and make public, without request, in all the geographical areas in which it operates, information about |
| | a) Audit processes; |
| | b) Processes for granting, refusing, maintaining, renewing, suspending, restoring or withdrawing certification or expanding or reducing the scope of certification; |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | c) Types of management systems and certification schemes in which it operates; |
| | d) The use of the certification body's name and certification mark or logo; |
| | e) Processes for handling requests for information, complaints and appeals; |
| | f ) Policy on impartiality. |
| 8.1.2 | The certification body shall provide upon request information about: |
| | a) Geographical areas in which it operates; |
| | b) The status of a given certification; |
| | c) The name, related normative document, scope and geographical location (city and country) for a specific certified client. |
| | **Note** 1: In exceptional cases, access to certain information can be limited on the request of the client (e.g. for security reasons). |
| | **Note** 2: The certification body can also make the information in 8.1.2 public by any means it chooses without request, e.g. on its internet website. |
| 8.1.3 | Information provided by the certification body to any client or to the marketplace, including advertising, shall be accurate and not misleading. |
| **8.2** | **Certification documents** |
| 8.2.1 | The certification body shall provide by any means it chooses certification documents to the certified client. |
| IS 8.2.1 | **IS 8.2 ISMS Certification documents** |
| | The certification documents may reference national and international standards as source(s) of control set for controls that are determined as necessary in the organization's Statement of Applicability in accordance with IS/ISO/IEC 27001:2013, 6.1.3 d). The reference on the certification documents shall be clearly stated as being only a control set source for controls applied in the Statement of Applicability and not a certification thereof. |
| CS-L3 | **IS 8.2 CSMS Certification documents** |
| | The certification documents may reference national and international standards as source(s) of control set for controls that are determined as necessary in the organization's Statement of Applicability in accordance with ATC (Level 3). The |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | reference on the certification documents shall be clearly stated as being only a control set source for controls applied in the Statement of Applicability and not a certification thereof. |
| 8.2.2 | **The certification document(s) shall identify the following:** |
| | a) The name and geographical location of each certified client (or the geographical location of the headquarters and any sites within the scope of a multi-site certification); |
| | b) The effective date of granting, expanding or reducing the scope of certification, or renewing certification which shall not be before the date of the relevant certification decision; |
| | **Note** The certification body can keep the original certification date on the certificate when a certificate lapses for a period of time provided that: |
| | — the current certification cycle start and expiry date are clearly indicated; |
| | — the last certification cycle expiry date be indicated along with the date of recertification audit. |
| | c) The expiry date or recertification due date consistent with the recertification cycle; |
| | d) A unique identification code; |
| | e) The management system standard and/or other normative document, including indication of issue status (e.g. revision date or number) used for audit of the certified client; |
| | f ) The scope of certification with respect to the type of activities, products and services as applicable at each site without being misleading or ambiguous; |
| | g) The name, address and certification mark of the certification body; other marks (e.g. accreditation symbol, client's logo) may be used provided they are not misleading or ambiguous; |
| | h) Any other information required by the standard and/or other normative document used for certification; |
| | i) In the event of issuing any revised certification documents, a means to distinguish the revised documents from any prior obsolete documents. |
| **8.3** | **Reference to certification and use of marks** |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| 8.3.1 | A certification body shall have rules governing any management system certification mark that it authorizes certified clients to use. These rules shall ensure, among other things, traceability back to the certification body. There shall be no ambiguity in the mark or accompanying text, as to what has been certified and which certification body has granted the certification. This mark shall not be used on a product nor product packaging nor in any other way that may be interpreted as denoting product conformity. |
| | **Note** IS/ISO/IEC 17030 provides additional information for use of third-party marks. |
| 8.3.2 | A certification body shall not permit its marks to be applied by certified clients to laboratory test, calibration or inspection reports or certificates. |
| 8.3.3 | A certification body shall have rules governing the use of any statement on product packaging or in accompanying information that the certified client has a certified management system. Product packaging is considered as that which can be removed without the product disintegrating or being damaged. Accompanying information is considered as separately available or easily detachable. Type labels or identification plates are considered as part of the product. The statement shall in no way imply that the product, process, or service is certified by this means. The statement shall include reference to: |
| | —identification (e.g., brand or name) of the certified client; |
| | —the type of management system (e.g., quality, environment) and the applicable standard; |
| | —the certification body issuing the certificate. |
| 8.3.4 | The certification body shall through legally enforceable arrangements require that the certified client: |
| | a) Conforms to the requirements of the certification body when making reference to its certification status in communication media such as the internet, brochures or advertising, or other documents; |
| | b) Does not make or permit any misleading statement regarding its certification; |
| | c) Does not use or permit the use of a certification document or any part thereof in a misleading manner; |
| | d) Upon withdrawal of its certification, discontinues its use of all advertising matter that contains a reference to certification, as directed by the certification body (see 9.6.5); |
| | e) Amends all advertising matter when the scope of certification has been reduced; |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | f) Does not allow reference to its management system certification to be used in such a way as to imply that the certification body certifies a product (including service) or process; |
| | g) Does not imply that the certification applies to activities and sites that are outside the scope of certification; |
| | h) Does not use its certification in such a manner that would bring the certification body and/or certification system into disrepute and lose public trust. |
| 8.3.5 | The certification body shall exercise proper control of ownership and shall take action to deal with incorrect references to certification status or misleading use of certification documents, marks or audit reports. |
| | **Note** Such action could include requests for correction and corrective action, suspension, withdrawal of certification, publication of the transgression and, if necessary, legal action. |
| **8.4** | **Confidentiality** |
| 8.4.1 | The certification body shall be responsible, through legally enforceable agreements, for the management of all information obtained or created during the performance of certification activities at all levels of its structure, including committees and external bodies or individuals acting on its behalf. |
| IS 8.4.1 | **IS 8.4 Access to organisational records** |
| | Before the certification audit, the certification body shall ask the client to report if any ISMS related information (such as ISMS records or information about design and effectiveness of controls) cannot be made available for review by the audit team because it contains confidential or sensitive information. The certification body shall determine whether the ISMS can be adequately audited in the absence of such information. If the certification body concludes that it is not possible to adequately audit the ISMS without reviewing the identified confidential or sensitive information, it shall advise the client that the certification audit cannot take place until appropriate access arrangements are granted. |
| CS-L3 | **IS 8.4 Access to organizational records** |
| | Before the certification audit, the certification body shall ask the client to report if any CSMS related information (such as CSMS records or information about design and effectiveness of controls) cannot be made available for review by the audit team because it contains confidential or sensitive information. The certification body shall determine whether the CSMS can be adequately audited in the absence of such information. If the certification body concludes that it is not possible to adequately audit the ISMS without |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | reviewing the identified confidential or sensitive information, it shall advise the client that the certification audit cannot take place until appropriate access arrangements are granted. |
| 8.4.2 | The certification body shall inform the client, in advance, of the information it intends to place in the public domain. All other information, except for information that is made publicly accessible by the client, shall be considered confidential. |
| 8.4.3 | Except as required in this part of IS/ISO/IEC 17021, information about a particular certified client or individual shall not be disclosed to a third party without the written consent of the certified client or individual concerned. |
| 8.4.4 | When the certification body is required by law or authorized by contractual arrangements (such as with the accreditation body) to release confidential information, the client or individual concerned shall, unless prohibited by law, be notified of the information provided. |
| 8.4.5 | Information about the client from sources other than the client (e.g., complainant, regulators) shall be treated as confidential, consistent with the certification body's policy. |
| 8.4.6 | 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 except as required by law. |
| 8.4.7 | The certification body shall have processes and where applicable equipment and facilities that ensure the secure handling of confidential information. |
| **8.5** | **Information exchange between a certification body and its clients** |
| 8.5.1 | Information on the certification activity and requirements |
| | The certification body shall provide information and update clients on the following: |
| | a) A detailed description of the initial and continuing certification activity, including the application, initial audits, surveillance audits, and the process for granting, refusing, maintaining of certification, expanding or reducing the scope of certification, renewing, suspending or restoring, or withdrawing of certification; |
| | b) The normative requirements for certification; |
| | c) Information about the fees for application, initial certification, and continuing certification; |
| | d) The certification body's requirements for clients to: |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | 1) Comply with certification requirements; |
| | 2) Make all necessary arrangements for the conduct of the audits, including provision for examining documentation and the access to all processes and areas, records and personnel for the purposes of initial certification, surveillance, recertification and resolution of complaints; |
| | 3) Make provisions, where applicable, to accommodate the presence of observers (e.g. accreditation assessors or trainee auditor); |
| | e) Documents describing the rights and duties of certified clients, including requirements, when making reference to its certification in communication of any kind in line with the requirements in 8.3; |
| | f) Information on processes for handling complaints and appeals. |
| 8.5.2 | **Notice of changes by a certification body** |
| | The certification body shall give its certified clients due notice of any changes to its requirements for certification. The certification body shall verify that each certified client complies with the new requirements. |
| 8.5.3 | **Notice of changes by a certified client** |
| | The certification body shall have legally enforceable arrangements to ensure that the certified client informs the certification body, without delay, of matters that may affect the capability of the management system to continue to fulfil the requirements of the standard used for certification. These include, for example, changes relating to: |
| | a) The legal, commercial, organizational status or ownership; |
| | b) Organisation and management (e.g. key managerial, decision-making or technical staff ); |
| | c) Contact address and sites; |
| | d) Scope of operations under the certified management system; |
| | e) Major changes to the management system and processes. |
| | The certification body shall take action as appropriate. |
| **9** | **Process requirements** |
| **9.1** | **Pre-certification activities** |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| 9.1.1 | **Application** |
| | The certification body shall require an authorized representative of the applicant organisation to provide the necessary information to enable it to establish the following: |
| | a) The desired scope of the certification; |
| | b) Relevant details of the applicant organization as required by the specific certification scheme, including its name and the address(es) of its site(s), its processes and operations, human and technical resources, functions, relationships and any relevant legal obligations; |
| | c) Identification of outsourced processes used by the organization that will affect conformity to requirements; |
| | d) The standards or other requirements for which the applicant organization is seeking certification; |
| | e) Whether consultancy relating to the management system to be certified has been provided and, if so, by whom. |
| IS 9.1.1.1 | **IS 9.1.1 Application readiness** |
| | The certification body shall require the client to have a documented and implemented ISMS which conforms to IS/ISO/IEC 27001 and other documents required for certification |
| CS-L3 | **IS 9.1.1 Application readiness** |
| | The certification body shall require the client to have a documented and implemented CSMS which conforms to ATC (Level 3) and other documents required for certification |
| **9.1.2** | **Application review** |
| 9.1.2.1 | The certification body shall conduct a review of the application and supplementary information for certification to ensure that: |
| | a) The information about the applicant organization and its management system is sufficient to develop an audit program (see 9.1.3); |
| | b) Any known difference in understanding between the certification body and the applicant organization is resolved; |
| | c) The certification body has the competence and ability to perform the certification activity; |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | d) The scope of certification sought, the site(s) of the applicant organization's operations, time required to complete audits and any other points influencing the certification activity are taken into account (language, safety conditions, threats to impartiality, etc.). |
| 9.1.2.2 | The following the review of the application, the certification body shall either accept or decline an application for certification. When the certification body declines an application for certification as a result of the review of application, the reasons for declining an application shall be documented and made clear to the client. |
| 9.1.2.3 | Based on this review, the certification body shall determine the competences it needs to include in its audit team and for the certification decision. |
| CS-L3 | At the time of application review, the TL shall focus on SoA, DRR and implementation of compensating countermeasures. The TL shall take into the cognisance of various certified and components and sub systems are used. These can be from any CB signatory to Multi-lateral agreement of IAF. |
| **9.1.3** | **Audit programme** |
| 9.1.3.1 | An audit programme for the full certification cycle shall be developed to clearly identify the audit activity/activities required to demonstrate that the client's management system fulfils the requirements for certification to the selected standard(s) or other normative document(s). The audit programme for the certification cycle shall cover the complete management system requirements. |
| 9.1.3.2 | The audits programme for the initial certification shall include a two-stage initial audit, surveillance audits in the first and second years following the certification decision, and a recertification audit in the third year prior to expiration of certification. The first three-year certification cycle begins with the certification decision. Subsequent cycles begin with the recertification decision (see 9.6.3.2.3) The determination of the audit programme and any subsequent adjustments shall consider the size of the client, the scope and complexity of its management system, products and processes as well as demonstrated level of management system effectiveness and the results of any previous audits. |
| | **Note**1 Annex E provides a flowchart of a typical audit and certification process. |
| | **Note** 2 The following list contains additional items that can be considered when developing or revising an audit |
| | programme, they might also need to be addressed when determining the audit scope and developing the audit plan: |
| | — complaints received by the certification body about the client; |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | — combined, integrated or joint audit |
| | — changes to the certification requirements; |
| | — changes to legal requirements; |
| | — changes to accreditation requirements; |
| | — organisational performance data (e.g. defect levels, key performance indicators data); |
| | — relevant interested parties' concerns. |
| | **Note** 3 If specified by the industry specific certification scheme, the certification cycle can be different from three years. |
| IS 9.1.3.2 | **IS 9.1.3 Audit Methodology** |
| | The certification body's procedures shall not presuppose a particular manner of implementation of an ISMS or a particular format for documentation and records. Certification procedures shall focus on establishing that a client's ISMS meets the requirements specified in IS/ISO/IEC 27001 and the policies and objectives of the client. |
| | **Note** Further guidance on auditing is given in IS/ISO/IEC 27007 |
| CS-L3 | **IS 9.1.3 Audit Methodology** |
| | The certification body's procedures shall not presuppose a particular manner of implementation of an CSMS or a particular format for documentation and records. Certification procedures shall focus on establishing that a client's CSMS meets the requirements specified in ATC (Level 3) and the policies and objectives of the client. |
| 9.1.3.3 | Surveillance audits shall be conducted at least once a calendar year, except in recertification years. The date of the first surveillance audit following initial certification shall not be more than 12 months from the certification decision date. |
| | **Note** It can be necessary to adjust the frequency of surveillance audits to accommodate factors such as seasons or management systems certification of a limited duration (e.g. temporary construction site). |
| IS 9.1.3.3 | **IS 9.1.3 General preparations for the initial audit** |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | The certification body shall require that a client makes all necessary arrangements for the access to internal audit reports and reports of independent reviews of information security. |
| | At least the following information shall be provided by the client during stage 1 of the certification audit: |
| | a) General information concerning the ISMS and the activities it covers; |
| | b) A copy of the required ISMS documentation specified in IS/ISO/IEC 27001 and, where required, associated documentation |
| CS-L3 | a) General information concerning the CSMS and the activities it covers; |
| | b) A copy of the required CSMS and associated documentation. |
| 9.1.3.4 | Where the certification body is taking account of certification already granted to the client and to audits performed by another certification body, it shall obtain and retain sufficient evidence, such as reports and documentation on corrective actions, to any nonconformity. The documentation shall support the fulfilling of the requirements in this part of IS/ISO/IEC 17021. The certification body shall, based on the information obtained, justify and record any adjustments to the existing audit programme and follow up the implementation of corrective actions concerning previous nonconformities. |
| IS 9.1.3.4 | **IS 9.1.3 Review periods** |
| | The certification body shall not certify an ISMS unless it has been operated through at least one management review and one internal ISMS audit covering the scope of certification |
| 9.1.3.5 | Where the client operates shifts, the activities that take place during shift working shall be considered when developing the audit programme and audit plans. |
| CS-L3 | **IS 9.1.3 Review periods** |
| | The certification body shall not certify an CSMS unless it has been operated through at least one management review and one internal CSMS audit covering the scope of certification |
| | Where the client operates shifts, the activities that take place during shift working shall be considered when developing the audit programme and audit plans. |
| IS 9.1.3.5 | **IS 9.1.3 Scope of certification** |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | The audit team shall audit the ISMS of the client covered by the defined scope against all applicable certification requirements. The certification body shall confirm, in the scope of the client ISMS, that clients address the requirements stated in IS/ISO/IEC 27001, 4.3. |
| | Certification bodies shall ensure that the client's information security risk assessment and risk treatment properly reflects its activities and extends to the boundaries of its activities as defined in the scope of certification. Certification bodies shall confirm that this is reflected in the client's scope of their ISMS and Statement of Applicability. The certification body shall verify that there is at least one Statement of Applicability per scope of certification. |
| | Certification bodies shall ensure that interfaces with services or activities that are not completely within the scope of the ISMS are addressed within the ISMS subject to certification and are included in the client's information security risk assessment. An example of such a situation is the sharing of facilities (e.g. IT systems, databases and telecommunication systems or the outsourcing of a business function) with other organizations |
| CS-L3 | **IS 9.1.3 Scope of certification** |
| | The audit team shall audit the CSMS of the client covered by the defined scope against all applicable certification requirements. The certification body shall confirm, in the scope of the client CSMS, that clients address the requirements stated in ATC (Level 3). |
| | Certification bodies shall ensure that the client's information security risk assessment and risk treatment properly reflects its activities and extends to the boundaries of its activities as defined in the scope of certification. Certification bodies shall confirm that this is reflected in the client's scope of their CSMS and Statement of Applicability. The certification body shall verify that there is at least one Statement of Applicability per scope of certification. |
| | Certification bodies shall ensure that interfaces with services or activities that are not completely within the scope of the CSMS are addressed within the ISMS subject to certification and are included in the client's information security risk assessment. An example of such a situation is the sharing of facilities (e.g. IT systems, databases and telecommunication systems or the outsourcing of a business function) with other organisations |
| ***IS 9.1.3.6*** | **IS 9.1.3 Certification audit criteria** |
| | The criteria against which the ISMS of a client is audited shall be the ISMS standard IS/ISO/IEC 27001. Other documents may be required for certification relevant to the function performed |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| **CS-L3** | **IS 9.1.3 Certification audit criteria** |
| | The criteria against which the CSMS of a client is audited shall be the CSMS standard ATC (Level 3). Other documents may be required for certification relevant to the function performed. |
| **9.1.4** | **Determining audit time** |
| 9.1.4.1 | The certification body shall have documented procedures for determining audit time. For each client the certification body shall determine the time needed to plan and accomplish a complete and effective audit of the client's management system. |
| CS-L3 | Refer to Annex A titled as 'Audit Duration' mentioned in Section 4 of this document. |
| IS 9.1.4.1 | **IS 9.1.4 Audit time** |
| | Certification bodies shall allow auditors sufficient time to undertake all activities relating to an initial audit, surveillance audit or re-certification audit. The calculation of overall audit time shall include sufficient time for audit reporting. |
| | The certification body shall use Annex B to determine audit time. |
| | Refer to changes in B2.1, B3.6 and B.6 as per Amendment 1 of ISO 27006:2015 |
| | **Note** Further guidance and examples on audit time calculation are provided in Annex C |
| 9.1.4.2 | In determining the audit time, the certification body shall consider, among other things, the |
| | following aspects: |
| | a) The requirements of the relevant management system standard; |
| | b) Complexity of the client and its management system; |
| | c) Technological and regulatory context; |
| | d) Any outsourcing of any activities included in the scope of the management system; |
| | e) The results of any prior audits; |
| | f ) Size and number of sites, their geographical locations and multi-site considerations; |
| | g) The risks associated with the products, processes or activities of the organization; |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | h) Whether audits are combined, joint or integrated. |
| | **Note** 1 : Time spent travelling to and from audited sites is not included in the calculation of the duration of the management system audit days. |
| | **Note** 2 : The certification body can use the guidelines established in IS/ISO/IEC TS 17023 for determining the duration of management system audit when documenting these procedures. |
| | Where specific criteria have been established for a specific certification scheme, e.g. ISO/TS 22003 or |
| | IS/ISO/IEC 27006, these shall be applied. |
| 9.1.4.3 | The duration of the management system audit and its justification shall be recorded. |
| 9.1.4.4 | The time spent by any team member that is not assigned as an auditor (i.e. technical experts, translators, interpreters, observers and auditors-in-training) shall not count in the above established duration of the management system audit. |
| | **Note** The use of translators and interpreters can necessitate additional time. |
| 9.1.5 | **Multi-site sampling** |
| | Where multi-site sampling is used for the audit of a client's management system covering the same activity in various geographical locations, the certification body shall develop a sampling programme to ensure proper audit of the management system. The rationale for the sampling plan shall be documented for each client. Sampling is not allowed for some specific certification schemes, and where specific criteria have been established for a specific certification scheme, e.g. ISO/TS 22003, these shall be applied. |
| | **Note** Where there are multiple sites not covering the same activity sampling is not appropriate. |
| CS-L3 | For the initial audit, all the sites of CSEs shall be audited. |
| IS 9.1.5.1 | **IS 9.1.5 Multiple Sites** |
| | Where a client has a number of sites meeting the criteria from a) to c) below, certification bodies may consider using a sample-based approach to multiple-site certification audit: |
| | a) All sites are operating under the same ISMS, which is centrally administered and audited and subject to central management review; |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | b) All sites are included within the client's internal ISMS audit programme; |
| | c) All sites are included within the client's ISMS management review programme |
| IS 9.1.5.1.2 | The certification body wishing to use a sample-based approach shall have procedures in place to ensure the following: |
| | a) The initial contract review identifies, to the greatest extent possible, the difference between sites such that an adequate level of sampling is determined |
| | b) A representative number of sites have been sampled by the certification body, taking into account: |
| | 1) The results of internal audits of the head office and the sites; |
| | 2) The results of management review; |
| | 3) Variations in the size of the sites; |
| | 4) Variations in the business purpose of the sites; |
| | 5) Complexity of the information systems at the different sites; |
| | 6) Variations in working practices; |
| | 7) Variations in activities undertaken; |
| | 8) Variations of design and operation of controls; |
| | 9) Potential interaction with critical information systems or information systems processing sensitive information; |
| | 10) Any differing legal requirements; |
| | 11) Geographical and cultural aspects; |
| | 12) Risk situation of the sites; |
| | 13) Information security incidents at the specific sites |
| | c) A representative sample is selected from all sites within the scope of the client's ISMS; this selection shall be based upon judgmental choice to reflect the factors presented in item b) above as well as a random element. |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | CS-L3: A representative sample is selected from all sites within the scope of the client's CSMS; this selection shall be based upon judgmental choice to reflect the factors presented in item b) above as well as a random element. |
| | d) Every site included in the ISMS which is subject to significant risks is audited by the certification body prior to certification. |
| | CS-L3: Every site included in the CSMS which is subject to significant risks is audited by the certification body prior to certification. |
| | e) The audit programme has been designed in the light of the above requirements and covers representative samples of the scope of the ISMS certification within the three year period. |
| | CS-L3: e) The audit programme has been designed in the light of the above requirements and covers representative samples of the scope of the CSMS certification within the three year period. |
| | f) In the case of a nonconformity being observed, either at the head office or at a single site, the corrective action procedure applies to the head office and all sites covered by the certificate. |
| | The audit shall address the client's head office activities to ensure that a single ISMS applies to all sites and delivers central management at the operational level. The audit shall address all the issues outlined above |
| CS-L3 | The audit shall address the client's head office activities to ensure that a single CSMS applies to all sites and delivers central management at the operational level. The audit shall address all the issues outlined above |
| 9.1.6 | When certification to multiple management system standards is being provided by the certification body, the planning for the audit shall ensure adequate on-site auditing to provide confidence in the certification. |
| **IS 9.1.6.1** | **IS 9.1.6 Integration of ISMS documentation with that for other management systems** |
| | The certification body may accept documentation that is combined (e.g. for information security, quality, health and safety and environment) as long as the ISMS can be clearly identified together with the appropriate interfaces to the other systems |
| **CS-L3** | **IS 9.1.6 Integration of CSMS documentation with that for other management systems** |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | The certification body may accept documentation that is combined (e.g. for information security, quality, health and safety and environment) as long as the CSMS can be clearly identified together with the appropriate interfaces to the other systems |
| **IS 9.1.6.2** | **IS 9.1.6 Combining management system audits** |
| | The ISMS audit may be combined with audits of other management systems, provided that it can be demonstrated that the audit satisfies all requirements for certification of the ISMS. All the elements important to an ISMS shall appear clearly and be readily identifiable in the audit reports. The quality of the audit shall not be adversely affected by the combination of the audits. |
| **CS-L3** | **IS 9.1.6 Combining management system audits** |
| | The CSMS ATC (Level 3) audit may be combined with audits of other management systems, provided that it can be demonstrated that the audit satisfies all requirements for certification of the CSMS. All the elements important to an CSMS shall appear clearly and be readily identifiable in the audit reports. The quality of the audit shall not be adversely affected by the combination of the audits. |
| **9.2** | **Planning audits** |
| **9.2.1** | Determining audit objectives, scope and criteria |
| 9.2.1.1 | The audit objectives shall be determined by the certification body. The audit scope and criteria, including any changes, shall be established by the certification body after discussion with the client. |
| IS 9.2.1.1 | **IS 9.2.1 Audit objectives** |
| | The audit objectives shall include the determination of the effectiveness of the management system to ensure that the client, based on the risk assessment, has implemented applicable controls and achieved the established information security objectives |
| 9.2.1.2 | The audit objectives shall describe what is to be accomplished by the audit and shall include the following: |
| | a) Determination of the conformity of the client's management system, or parts of it, with audit criteria; |
| | b) Determination of the ability of the management system to ensure the client meets applicable statutory, regulatory and contractual requirements; |
| | **Note** A management system certification audit is not a legal compliance audit. |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | c) Determination of the effectiveness of the management system to ensure the client can reasonably expect to achieving its specified objectives; |
| | d) As applicable, identification of areas for potential improvement of the management system. |
| 9.2.1.3 | The audit scope shall describe the extent and boundaries of the audit, such as sites, organisational units, activities and processes to be audited. Where the initial or re-certification process consists of more than one audit (e.g. covering different sites), the scope of an individual audit may not cover the full certification scope, but the totality of audits shall be consistent with the scope in the certification document. |
| 9.2.1.4 | The audit criteria shall be used as a reference against which conformity is determined, and |
| | shall include: |
| | —the requirements of a defined normative document on management systems; |
| | —the defined processes and documentation of the management system developed by the client. |
| **9.2.2** | **Audit team selection and assignments (refer to Note 2)** |
| **9.2.2.1** | **General** |
| IS 9.2.2.1 | **IS 9.2.2 Audit team:** |
| | The audit team shall be formally appointed and provided with the appropriate working documents. The mandate given to the audit team shall be clearly defined and made known to the client. |
| | An audit team may consist of one person provided that the person meets all the criteria set out in 7.1.2.1. |
| CS-L3 | All audit team members shall have police verification and background checks and records shall be maintained. AB may conduct Knowledge and Skill test of auditor(s) and technical expert(s), as deemed fit, to ascertain the competency required by personnel of CBs. Refer to the competency requirements mentioned in Annex B of this section. |
| 9.2.2.1.1 | The certification body shall have a process for selecting and appointing the audit team, including the audit team leader and technical experts as necessary, taking into account the competence needed to achieve the objectives of the audit and requirements for impartiality. If there is only one auditor, the auditor shall have the competence to perform |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | the duties of an audit team leader applicable for that audit. The audit team shall have the totality of the competences identified by the certification body as set out in 9.1.2.3 for the audit. |
| 9.2.2.1.2 | In deciding the size and composition of the audit team, consideration shall be given to the following: |
| | a) Audit objectives, scope, criteria and estimated audit time; |
| | b) Whether the audit is a combined, joint or integrated; |
| | c) The overall competence of the audit team needed to achieve the objectives of the audit (see Table A.1); |
| | d) Certification requirements (including any applicable statutory, regulatory or contractual requirements); |
| | e) Language and culture. |
| | **Note** The team leader of a combined or integrated audit is expected to have in-depth knowledge of at least one of the standards and an awareness of the other standards used for that particular audit. |
| 9.2.2.1.3 | The necessary knowledge and skills of the audit team leader and auditors may be supplemented by technical experts, translators and interpreters who shall operate under the direction of an auditor. Where translators or interpreters are used, they shall be selected such that they do not unduly influence the audit. |
| | **Note** The criteria for the selection of technical experts are determined on a case-by-case basis by the needs of the audit team and the scope of the audit. |
| 9.2.2.1.4 | Auditors-in-training may participate in the audit, provided an auditor is appointed as an evaluator. The evaluator shall be competent to take over the duties and have final responsibility for the activities and findings of the auditor-in-training. |
| 9.2.2.1.5 | The audit team leader, in consultation with the audit team, shall assign to each team member responsibility for auditing specific processes, functions, sites, areas or activities. Such assignments shall take into account the need for competence, and the effective and efficient use of the audit team, as well as different roles and responsibilities of auditors, auditors-in-training and technical experts. Changes to the work assignments may be made as the audit progresses to ensure achievement of the audit objectives. |
| **9.2.2.2** | **Observers, technical experts and guides** |
| IS 9.2.2.2 | **IS 9.2.2 Audit team competence** |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | The requirements listed in 7.1.2 apply. For surveillance and special audit activities, only those requirements which are relevant to the scheduled surveillance activity and special audit activity apply. |
| | When selecting and managing the audit team to be appointed for a specific certification audit the certification body shall ensure that the competences brought to each assignment are appropriate. The team shall: |
| | a) Have appropriate technical knowledge of the specific activities within the scope of the ISMS for which certification is sought and, where relevant, with associated procedures and their potential information security risks (technical experts may fulfil this function); |
| | CS-L3: a) Have appropriate technical knowledge of the specific activities within the scope of the CSMS for which certification is sought and, where relevant, with associated procedures and their potential information security risks (technical experts may fulfil this function); |
| | b) Have understanding of the client sufficient to conduct a reliable certification audit of its ISMS given the ISMS' scope and context within the organization in managing the information security aspects of its activities, products and services; |
| | CS-L3: b) Have understanding of the client sufficient to conduct a reliable certification audit of its CSMS given the CSMS' scope and context within the organization in managing the information security aspects of its activities, products and services; |
| | c) Have appropriate understanding of the legal and regulatory requirements applicable to the client's ISMS. |
| | CS-L3: c) Have appropriate understanding of the legal and regulatory requirements applicable to the client's CSMS. |
| | **Note** Appropriate understanding does not imply a profound legal background |
| CS-L3 | The CSE may review critically before agreeing that technical experts can be from TB, CO, Academia or from competing industry and empanelled by a CB and claiming that they meet the requirements of confidentiality and integrity. |
| 9.2.2.2.1 | **Observers** |
| | The presence and justification of observers during an audit activity shall be agreed to by the certification body and client prior to the conduct of the audit. The audit team shall ensure that observers do not unduly influence or interfere in the audit process or outcome of the audit. |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | **Note** Observers can be members of the client's organization, consultants, witnessing accreditation body personnel, regulators or other justified persons. |
| CS-L3 | CSEs having CII should review critically the presence of observers and allow if there is a compelling reason after documenting the same and obtaining the approval of the management. |
| 9.2.2.2.2 | **Technical experts** |
| | The role of technical experts during an audit activity shall be agreed to by the certification body and client prior to the conduct of the audit. A technical expert shall not act as an auditor in the audit team. The technical experts shall be accompanied by an auditor. |
| | **Note** The technical experts can provide advice to the audit team for the preparation, planning or audit. |
| CS-L3 | Technical experts shall meet the requirements as specified in Annex B of this section. |
| 9.2.2.2.3 | **Guides** |
| | Each auditor shall be accompanied by a guide, unless otherwise agreed to by the audit team leader and the client. Guide(s) are assigned to the audit team to facilitate the audit. The audit team shall ensure that guides do not influence or interfere in the audit process or outcome of the audit. |
| | NOTE 1 : The responsibilities of a guide can include: |
| | a) Establishing contacts and timing for interviews; |
| | b) Arranging visits to specific parts of the site or organization; |
| | c) Ensuring that rules concerning site safety and security procedures are known and respected by the audit team members; |
| | d) Witnessing the audit on behalf of the client; |
| | e) Providing clarification or information as requested by an auditor. |
| | **Note 2 :** Where appropriate, the auditee can also act as the guide. |
| **9.2.3** | **Audit Plan** |
| 9.2.3.1 | **General** |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | The certification body shall ensure that an audit plan is established prior to each audit identified in the audit programme to provide the basis for agreement regarding the conduct and scheduling of the audit activities. |
| | **Note** It is not expected that a certification body will develop an audit plan for each audit at the time that the audit programme is developed. |
| 9.2.3.2 | **Preparing the audit plan** |
| | The audit plan shall be appropriate to the objectives and the scope of the audit. The audit plan shall at least include or refer to the following: |
| | a) The audit objectives; |
| | b) The audit criteria; |
| | c) The audit scope, including identification of the organizational and functional units or processes to be audited; |
| | d) The dates and sites where the on-site audit activities will be conducted, including visits to temporary sites and remote auditing activities, where appropriate; |
| | e) The expected duration of on-site audit activities; |
| | f) The roles and responsibilities of the audit team members and accompanying persons, such as observers or interpreters. |
| | NOTE The audit plan information can be addresses in more than one document. |
| IS 9.2.3.2 | **IS 9.2.3 Network-assisted audit techniques** |
| | The audit plan shall identify the network-assisted auditing techniques that will be utilized during the audit, as appropriate. |
| | Network assisted auditing techniques may include, for example, teleconferencing, web meeting, interactive web-based communications and remote electronic access to the ISMS documentation or ISMS processes. The focus of such techniques should be to enhance audit effectiveness and efficiency and should support the integrity of the audit process. |
| CS-L3 | Network assisted auditing techniques may include, for example, teleconferencing, web meeting, interactive web-based communications and remote electronic access to the CSMS documentation or CSMS processes. The focus of such techniques should be to enhance audit effectiveness and efficiency and should support the integrity of the audit process. |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| 9.2.3.3 | **Communication of audit team tasks** |
| | The tasks given to the audit team shall be defined, and require the audit team to: |
| | a) Examine and verify the structure, policies, processes, procedures, records and related documents of the client relevant to the management system standard; |
| | b) Determine that these meet all the requirements relevant to the intended scope of certification; |
| | c) Determine that the processes and procedures are established, implemented and maintained |
| | effectively, to provide a basis for confidence in the client's management system; |
| | d) Communicate to the client, for its action, any inconsistencies between the client's policy, objectives and targets. |
| IS 9.2.3.3 | **IS 9.2.3 Timing of audit:** |
| | A certification body should agree with the organisation to be audited the timing of the audit which will best demonstrate the full scope of the organization. The consideration could include season, month, day/dates and shift as appropriate. |
| 9.2.3.4 | **Communication of audit plan** |
| | The audit plan shall be communicated and the dates of the audit shall be agreed upon, in advance, with the client. |
| 9.2.3.5 | **Communication concerning audit team members** |
| | The certification body shall provide the name of and, when requested, make available background information on each member of the audit team, with sufficient time for the client to object to the appointment of any particular audit team member and for the certification body to reconstitute the team in response to any valid objection. |
| **9.3** | **Initial certification** |
| **9.3.1** | **Initial certification audit** |
| 9.3.1.1 | **General** |
| | The initial certification audit of a management system shall be conducted in two stages: stage 1 and stage 2. |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| IS 9.3.1.1 | **IS 9.3.1.1 Stage 1** |
| | In this stage of the audit the certification body shall obtain documentation on the design of the ISMS covering the documentation required in IS/ISO/IEC 27001. |
| | CS-L3: In this stage of the audit the certification body shall obtain documentation on the design of the CSMS covering the documentation required in ATC (Level 3). |
| | The certification body shall obtain a sufficient understanding of the design of the ISMS in the context of the client's organization, risk assessment and treatment (including the controls determined), information security policy and objectives and, in particular, of the client's preparedness for the audit. This allows planning for stage 2. |
| | The results of stage 1 shall be documented in a written report. The certification body shall review |
| | the stage 1 audit report before deciding on proceeding with stage 2 and shall confirm if the stage 2 audit team members have the necessary competence; this may be done by the auditor leading the team that conducted the stage 1 audit if deemed competent and appropriate. |
| | **Note** Independent review (i.e. by a person from the certification body not involved in the audit) is one |
| | measure to mitigate the risks involved when deciding if and with whom to proceed to stage 2. However, other risk mitigation measures can already be in place achieving the same goal. |
| | The certification body shall make the client aware of the further types of information and records that may be required for detailed examination during stage 2. |
| **9.3.1.2** | **Stage 1** |
| 9.3.1.2.1 | Planning shall ensure that the objectives of stage 1 can be met and the client shall be informed |
| | of any "on site" activities during stage 1. |
| | **Note** Stage 1 does not require a formal audit plan (see 9. 2.3). |
| IS 9.3.1.2 | **IS 9.3.1.2 Stage 2** |
| IS 9.3.1.2.1 | On the basis of findings documented in the stage 1 audit report, the certification body develops an audit plan for the conduct of stage 2. In addition to evaluating the effective implementation of the ISMS, the objectives of stage 2 are: |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | CS-L3: On the basis of findings documented in the stage 1 audit report, the certification body develops an audit plan for the conduct of stage 2. In addition to evaluating the effective implementation of the CSMS, the objectives of stage 2 are: |
| | a) To confirm that the client adheres to its own policies, objectives and procedures |
| 9.3.1.2.2 | The objectives of stage 1 are to: |
| | a) Review the client's management system documented information; |
| | b) Evaluate the client's site-specific conditions and to undertake discussions with the client's personnel to determine the preparedness for stage 2; |
| | c) Review the client's status and understanding regarding requirements of the standard, in particular with respect to the identification of key performance or significant aspects, processes, objectives and operation of the management system; |
| | d) Obtain necessary information regarding the scope of the management system, including: |
| | —the client's site(s); |
| | —processes and equipment used; |
| | —levels of controls established (particularly in case of multisite clients); |
| | —applicable statutory and regulatory requirements; |
| | e) Review the allocation of resources for stage 2 and agree the details of stage 2 with the client; |
| | f) Provide a focus for planning stage 2 by gaining a sufficient understanding of the client's management system and site operations in the context of the management system standard or other normative document; |
| | g) Evaluate if the internal audits and management reviews are being planned and performed, and that the level of implementation of the management system substantiates that the client is ready for stage 2. |
| | **Note** If at least part of stage 1 is carried out at the client's premises, this can help to achieve the objectives stated above. |
| IS 9.3.1.2.2 | To do this, the audit shall focus on the client's: |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | a) Top management leadership and commitment to information security policy and the information security objectives; |
| | b) Documentation requirements listed in IS/ISO/IEC 27001; |
| | CS-L3: b) Documentation requirements listed in ATC (Level 3); |
| | c) Assessment of information security related risks and that the assessments produce consistent, valid and comparable results if repeated; |
| | d) Determination of control objectives and controls based on the information security risk assessment and risk treatment processes; |
| | e) Information security performance and the effectiveness of the ISMS, evaluating against the information security objectives; |
| | CS-L3: e) Cyber security performance and the effectiveness of the CSMS, evaluating against the information security objectives; |
| | f) Correspondence between the determined controls, the Statement of Applicability and the results of the information security risk assessment and risk treatment process and the information security policy and objectives; |
| | CS-L3: f) Correspondence between the determined controls, the Statement of Applicability and the results of the cyber security risk assessment and risk treatment process and the cyber security policy and objectives; |
| | g) Implementation of controls (see Annex D of ISO 27006), taking into account the external and internal context and related risks, the organization's monitoring, measurement and analysis of information security processes and controls, to determine whether controls are implemented and effective and meet their stated information security objectives; |
| | CS-L3: g) Implementation of controls (see Annex D of ISO 27006), taking into account the external and internal context and related risks, the organization's monitoring, measurement and analysis of information security processes and controls, to determine whether controls are implemented and effective and meet their stated cyber security objectives; |
| | h) Programmes, processes, procedures, records, internal audits and reviews of the ISMS effectiveness to ensure that these are traceable to top management decisions and the information security policy and objectives |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | CS-L3: h) Programmes, processes, procedures, records, internal audits and reviews of the CSMS effectiveness to ensure that these are traceable to top management decisions and the information security policy and objectives |
| 9.3.1.2.3 | Documented conclusions with regard to fulfilment of the stage 1 objectives and the readiness for stage 2 shall be communicated to the client, including identification of any areas of concern that could be classified as a nonconformity during stage 2. |
| | **Note** The stage 1 output does not need to meet the full requirements of a report (see 9.4.8). |
| 9.3.1.2.4 | In determining the interval between stage 1 and stage 2, consideration shall be given to the needs of the client to resolve areas of concern identified during stage 1. The certification body may also need to revise its arrangements for stage 2. If any significant changes which would impact the management system occur, the certification body shall consider the need to repeat all or part of stage 1. The client shall be informed that the results of stage 1 may lead to postponement or cancellation of stage 2. |
| 9.3.1.3 | **Stage 2** |
| | The purpose of stage 2 is to evaluate the implementation, including effectiveness, of the client's management system. The stage 2 shall take place at the site(s) of the client. It shall include the auditing of at least the following: |
| | a) Information and evidence about conformity to all requirements of the applicable management system standard or other normative documents; |
| | b) Performance monitoring, measuring, reporting and reviewing against key performance objectives and targets (consistent with the expectations in the applicable management system standard or other normative document); |
| | c) The client's management system ability and its performance regarding meeting of applicable statutory, regulatory and contractual requirements; |
| | d) Operational control of the client's processes; |
| | e) Internal auditing and management review; |
| | f) Management responsibility for the client's policies. |
| 9.3.1.4 | **Initial certification audit conclusions** |
| | The audit team shall analyse all information and audit evidence gathered during stage 1 and stage 2 to review the audit findings and agree on the audit conclusions. |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| **9.4** | **Conducting audits** |
| **9.4.1** | **General** |
| | The certification body shall have a process for conducting on-site audits. This process shall include an opening meeting at the start of the audit and a closing meeting at the conclusion of the audit. |
| | Where any part of the audit is made by electronic means or where the site to be audited is virtual, the certification body shall ensure that such activities are conducted by personnel with appropriate competence. The evidence obtained during such an audit shall be sufficient to enable the auditor to take an informed decision on the conformity of the requirement in question. |
| | **Note** "On-site" audits can include remote access to electronic site(s) that contain(s) information that is relevant to the audit of the management system. Consideration can also be given to the use of electronic means for conducting audits. |
| IS 9.4.1 | **IS 9.4 General** |
| | The certification body shall have documented procedures for: |
| | a) The initial certification audit of a client's ISMS, in accordance with the provisions of IS/ISO/IEC 17021-1; |
| | b) Surveillance and re-certification audits of a client's ISMS in accordance with IS/ISO/IEC 17021-1 on a periodic basis for continuing conformity with relevant requirements and for verifying and recording that a client takes corrective action on a timely basis to correct all nonconformities |
| CS-L3 | **IS 9.4 General** |
| | The certification body shall have documented procedures for: |
| | a) The initial certification audit of a client's CSMS, in accordance with the provisions of IS/ISO/IEC 17021-1; |
| | b) Surveillance and re-certification audits of a client's CSMS in accordance with IS/ISO/IEC 17021-1 on a periodic basis for continuing conformity with relevant requirements and for verifying and recording that a client takes corrective action on a timely basis to correct all nonconformities |
| 9.4.2 | **Conducting the opening meeting** |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | A formal opening meeting, shall be held with the client's management and, where appropriate, those responsible for the functions or processes to be audited. The purpose of the opening meeting, usually conducted by the audit team leader, is to provide a short explanation of how the audit activities will be undertaken. The degree of detail shall be consistent with the familiarity of the client with the audit process and shall consider the following: |
| | a) Introduction of the participants, including an outline of their roles; |
| | b) Confirmation of the scope of certification; |
| | c) Confirmation of the audit plan (including type and scope of audit, objectives and criteria), any changes, and other relevant arrangements with the client, such as the date and time for the closing meeting, interim meetings between the audit team and the client's management; |
| | d) Confirmation of formal communication channels between the audit team and the client; |
| | e) Confirmation that the resources and facilities needed by the audit team are available; |
| | f) Confirmation of matters relating to confidentiality; |
| | g) Confirmation of relevant work safety, emergency and security procedures for the audit team; |
| | h) Confirmation of the availability, roles and identities of any guides and observers; |
| | i) The method of reporting, including any grading of audit findings; |
| | j) Information about the conditions under which the audit may be prematurely terminated; |
| | k) Confirmation that the audit team leader and audit team representing the certification body is responsible for the audit and shall be in control of executing the audit plan including audit activities and audit trails; |
| | l) Confirmation of the status of findings of the previous review or audit, if applicable; |
| | m) Methods and procedures to be used to conduct the audit based on sampling; |
| | n) Confirmation of the language to be used during the audit; |
| | o) Confirmation that, during the audit, the client will be kept informed of audit progress and any concerns; |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | p) Opportunity for the client to ask questions. |
| IS 9.4.2 | **IS 9.4 Specific elements of the ISMS audit** |
| | The certification body, represented by the audit team, shall: |
| | a) Require the client to demonstrate that the assessment of information security related risks is relevant and adequate for the ISMS operation within the ISMS scope; |
| | b) Establish whether the client's procedures for the identification, examination and evaluation of information security related risks and the results of their implementation are consistent with the client's policy, objectives and targets. |
| | The certification body shall also establish whether the procedures employed in risk assessment are sound and properly implemented. |
| CS-L3 | **IS 9.4 Specific elements of the CSMS audit** |
| | The certification body, represented by the audit team, shall: |
| | a) Require the client to demonstrate that the assessment of information security related risks is relevant and adequate for the CSMS operation within the CSMS ATC (Level 3) scope; |
| | b) Establish whether the client's procedures for the identification, examination and evaluation of cyber security related risks and the results of their implementation are consistent with the client's policy, objectives and targets. The specific requirements also covers foundational requirements, security level, requirements, requirement enhancements and compensating counter measures. |
| | The certification body shall also "stab'lsh whether the procedures employed in risk assessment are sound and properly implemented. |
| 9.4.3 | **Communication during the audit** |
| 9.4.3.1 | During the audit, the audit team shall periodically assess audit progress and exchange information. The audit team leader shall reassign work as needed between the audit team members and periodically communicate the progress of the audit and any concerns to the client. |
| IS 9.4.3 | **IS 9.4 Audit report** |
| IS 9.4.3.1 | In addition to the requirements for reporting in IS/ISO/IEC 17021-1, 9.4.8, the audit report shall provide the following information or a reference to it: |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | a) An account of the audit including a summary of the document review; |
| | b) An account of the certification audit of the client's information security risk analysis; |
| | c) Deviations from the audit plan (e.g. more or less time spent on certain scheduled activities); |
| | d) The ISMS' scope |
| | CS-L3: d) the CSMS' scope |
| 9.4.3.2 | Where the available audit evidence indicates that the audit objectives are unattainable or suggests the presence of an immediate and significant risk (e.g. safety), the audit team leader shall report this to the client and, if possible, to the certification body to determine appropriate action. Such action may include reconfirmation or modification of the audit plan, changes to the audit objectives or audit scope, or termination of the audit. The audit team leader shall report the outcome of the action taken to the certification body. |
| IS 9.4.3.2 | The audit report shall be of sufficient detail to facilitate and support the certification decision. It shall contain: |
| | a) Significant audit trails followed and audit methodologies utilized (see 9.1.3.2); |
| | b) Observations made, both positive (e.g. noteworthy features) and negative (e.g. potential nonconformities); |
| | c) Comments on the conformity of the client's ISMS with the certification requirements with a clear statement of nonconformity, a reference to the version of the Statement of Applicability and, where applicable, any useful comparison with the results of previous certification audits of the client. |
| | CS-L3: c) Comments on the conformity of the client's CSMS with the certification requirements with a clear statement of nonconformity, a reference to the version of the Statement of Applicability and, where applicable, any useful comparison with the results of previous certification audits of the client. |
| | Completed questionnaires, checklists, observations, logs, or auditor notes may form an integral part of the audit report. If these methods are used, these documents shall be submitted to the certification body as evidence to support the certification decision. Information about the samples evaluated during the audit shall be included in the audit report, or in other certification documentation. |
| | The report shall consider the adequacy of the internal organization and procedures adopted by the client to give confidence in the ISMS. |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | CS-L3: The report shall consider the adequacy of the internal organization and procedures adopted by the client to give confidence in the CSMS. |
| | In addition to the requirements for reporting in IS/ISO/IEC 17021-1, 9.4.8, the report shall cover: |
| | — A summary of the most important observations, positive as well as negative, regarding the implementation and effectiveness of the ISMS requirements and IS controls; |
| | CS-L3: — A summary of the most important observations, positive as well as negative, regarding the implementation and effectiveness of the CSMS requirements and IS controls; |
| | — The audit team's recommendation as to whether the client's ISMS should be certified or not, with information to substantiate this recommendation |
| | CS-L3: — The audit team's recommendation as to whether the client's CSMS should be certified or not, with information to substantiate this recommendation |
| 9.4.3.3 | The audit team leader shall review with the client any need for changes to the audit scope which becomes apparent as on-site auditing activities progress and report this to the certification body. |
| **9.4.4** | **Obtaining and verifying information** |
| 9.4.4.1 | During the audit, information relevant to the audit objectives, scope and criteria (including information relating to interfaces between functions, activities and processes) shall be obtained by appropriate sampling and verified to become audit evidence. |
| 9.4.4.2 | Methods to obtain information shall include, but are not limited to: |
| | a) Interviews; |
| | b) Observation of processes and activities; |
| | c) Review of documentation and records. |
| **9.4.5** | **Identifying and recording audit findings** |
| 9.4.5.1 | Audit findings summarizing conformity and detailing nonconformity shall be identified, classified and recorded to enable an informed certification decision to be made or the certification to be maintained. |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| 9.4.5.2 | Opportunities for improvement may be identified and recorded, unless prohibited by the requirements of a management system certification scheme. Audit findings, however, which are nonconformities, shall not be recorded as opportunities for improvement. |
| 9.4.5.3 | A finding of nonconformity shall be recorded against a specific requirement, and shall contain a clear statement of the nonconformity, identifying in detail the objective evidence on which the nonconformity is based. Nonconformities shall be discussed with the client to ensure that the evidence is accurate and that the nonconformities are understood. The auditor however shall refrain from suggesting the cause of nonconformities or their solution. |
| 9.4.5.4 | The audit team leader shall attempt to resolve any diverging opinions between the audit team and the client concerning audit evidence or findings, and unresolved points shall be recorded. |
| **9.4.6** | **Preparing audit conclusions** |
| | Under the responsibility of the audit team leader and prior to the closing meeting, the audit team shall: |
| | a) Review the audit findings, and any other appropriate information obtained during the audit, against the audit objectives and audit criteria and classify the nonconformities; |
| | b) Agree upon the audit conclusions, taking into account the uncertainty inherent in the audit process; |
| | c) Agree any necessary follow-up actions; |
| | d) Confirm the appropriateness of the audit programme or identify any modification required for future audits (e.g. scope of certification, audit time or dates, surveillance frequency, audit team competence). |
| **9.4.7** | **Conducting the closing meeting** |
| 9.4.7.1 | A formal closing meeting, where attendance shall be recorded, shall be held with the client's management and, where appropriate, those responsible for the functions or processes audited. The purpose of the closing meeting, usually conducted by the audit team leader, is to present the audit conclusions, including the recommendation regarding certification. Any nonconformities shall be presented in such a manner that they are understood, and the timeframe for responding shall be agreed. |
| | NOTE "Understood" does not necessarily mean that the nonconformities have been accepted by the client. |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| 9.4.7.2 | The closing meeting shall also include the following elements where the degree of detail shall be consistent with the familiarity of the client with the audit process: |
| | a) Advising the client that the audit evidence obtained was based on a sample of the information; thereby introducing an element of uncertainty; |
| | b) The method and timeframe of reporting, including any grading of audit findings; |
| | c) The certification body's process for handling nonconformities including any consequences relating to the status of the client's certification; |
| | d) The timeframe for the client to present a plan for correction and corrective action for any nonconformities identified during the audit; |
| | e) The certification body's post audit activities; |
| | f) Information about the complaint and appeal handling processes. |
| 9.4.7.3 | The client shall be given opportunity for questions. Any diverging opinions regarding the audit findings or conclusions between the audit team and the client shall be discussed and resolved where possible. Any diverging opinions that are not resolved shall be recorded and referred to the certification body. |
| **9.4.8** | **Audit Report** |
| 9.4.8.1 | The certification body shall provide a written report for each audit to the client. The audit team may identify opportunities for improvement but shall not recommend specific solutions. Ownership of the audit report shall be maintained by the certification body. |
| 9.4.8.2 | The audit team leader shall ensure that the audit report is prepared and shall be responsible for its content. The audit report shall provide an accurate, concise and clear record of the audit to enable an informed certification decision to be made and shall include or refer to the following: |
| | a) Identification of the certification body; |
| | b) The name and address of the client and the client's representative; |
| | c) The type of audit (e.g. initial, surveillance or recertification audit or special audits); |
| | d) The audit criteria; |
| | e) The audit objectives; |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | f) The audit scope, particularly identification of the organizational or functional units or processes audited and the time of the audit; |
| | g) Any deviation from the audit plan and their reasons; |
| | h) Any significant issues impacting on the audit programme; |
| | i) Identification of the audit team leader, audit team members and any accompanying persons; |
| | j) The dates and places where the audit activities (on site or offsite, permanent or temporary sites) were conducted; |
| | k) Audit findings (see 9.4.5), reference to evidence and conclusions, consistent with the requirements |
| | of the type of audit; |
| | l) Significant changes, if any, that affect the management system of the client since the last audit took place; |
| | m) Any unresolved issues, if identified; |
| | n) Where applicable, whether the audit is combined, joint or integrated; |
| | o) A disclaimer statement indicating that auditing is based on a sampling process of the available |
| | information; |
| | p) Recommendation from the audit team |
| | q) The audited client is effectively controlling the use of the certification documents and marks, if applicable; |
| | r) Verification of effectiveness of taken corrective actions regarding previously identified nonconformities, if applicable. |
| 9.4.8.3 | The report shall also contain: |
| | a) A statement on the conformity and the effectiveness of the management system together with a summary of the evidence relating to: |
| | —the capability of the management system to meet applicable requirements and expected outcomes; |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | —the internal audit and management review process; |
| | b) A conclusion on the appropriateness of the certification scope; |
| | c) Confirmation that the audit objectives have been fulfilled. |
| **9.4.9** | **Cause analysis of nonconformities** |
| | The certification body shall require the client to analyse the cause and describe the specific correction and corrective actions taken, or planned to be taken, to eliminate detected nonconformities, within a defined time. |
| **9.4.10** | **Effectiveness of corrections and corrective actions** |
| | The certification body shall review the corrections, identified causes and corrective actions submitted by the client to determine if these are acceptable. The certification body shall verify the effectiveness of any correction and corrective actions taken. The evidence obtained to support the resolution of nonconformities shall be recorded. The client shall be informed of the result of the review and verification. The client shall be informed if an additional full audit, an additional limited audit, or documented evidence (to be confirmed during future audits) will be needed to verify effective correction and corrective actions. |
| | NOTE: Verification of effectiveness of correction and corrective action can be carried out based on a review of documented information provided by the client, or where necessary, through verification on-site. Usually this activity is done by a member of the audit team. |
| **9.5** | **Certification decision** |
| **9.5.1** | **General** |
| S 9.5.1 | **IS 9.5 Certification decision** |
| | The certification decision shall be based, additionally to the requirements of IS/ISO/IEC 17021-1, on the certification recommendation of the audit team as provided in their certification audit report (see 9.4.3). |
| | The persons or committees that take the decision on granting certification should not normally overturn a negative recommendation of the audit team. If such a situation does arise, the certification body shall document and justify the basis for the decision to overturn the recommendation. |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | Certification shall not be granted to the client until there is sufficient evidence to demonstrate that arrangements for management reviews and internal ISMS audits have been implemented, are effective and will be maintained. |
| | CS-L3: Certification shall not be granted to the client until there is sufficient evidence to demonstrate that arrangements for management reviews and internal CSMS audits have been implemented, are effective and will be maintained. |
| 9.5.1.1 | The certification body shall ensure that the persons or committees that make the decisions for granting or refusing certification, expanding or reducing the scope of certification, suspending or restoring certification, withdrawing certification or renewing certification are different from those who carried out the audits. The individual(s) appointed to conduct the certification decision shall have appropriate competence. |
| 9.5.1.2 | The person(s) [excluding members of committees (see 6.1.4)] assigned by the certification body to make a certification decision shall be employed by, or shall be under legally enforceable arrangement with either the certification body or an entity under the organisational control of the certification body. A certification body's organizational control shall be one of the following: |
| | a) Whole or majority ownership of another entity by the certification body; |
| | b) Majority participation by the certification body on the board of directors of another entity; |
| | c) A documented authority by the certification body over another entity in a network of legal entities (in which the certification body resides), linked by ownership or board of director control. |
| | **Note** For governmental certification bodies, other parts of the same government can be considered to be "linked by ownership" to the certification body. |
| 9.5.1.3 | The persons employed by, or under contract with, entities under organizational control shall fulfil the same requirements of this part of IS/ISO/IEC 17021 as persons employed by, or under contract with, the certification body. |
| 9.5.1.4 | The certification body shall record each certification decision including any additional information or clarification sought from the audit team or other sources. |
| **9.5.1** | **IS 9.5 Certification decision** |
| | The certification decision shall be based, additionally to the requirements of IS/ISO/IEC 17021-1, on the certification recommendation of the audit team as provided in their certification audit report (see 9.4.3). |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | The persons or committees that take the decision on granting certification should not normally overturn a negative recommendation of the audit team. If such a situation does arise, the certification body shall document and justify the basis for the decision to overturn the recommendation. |
| | Certification shall not be granted to the client until there is sufficient evidence to demonstrate that arrangements for management reviews and internal ISMS audits have been implemented, are effective and will be maintained. |
| | CS-L3: Certification shall not be granted to the client until there is sufficient evidence to demonstrate that arrangements for management reviews and internal CSMS audits have been implemented, are effective and will be maintained. |
| **9.5.2** | **Actions prior to making a decision** |
| | The certification body shall have a process to conduct an effective review prior to making a decision for granting certification, expanding or reducing the scope of certification, renewing, suspending or restoring, or withdrawing of certification, including, that |
| | a) The information provided by the audit team is sufficient with respect to the certification requirements and the scope for certification; |
| | b) For any major nonconformities, it has reviewed, accepted and verified the correction and corrective actions; |
| | c) For any minor nonconformities it has reviewed and accepted the client's plan for correction and corrective action. |
| **9.5.3** | **Information for granting initial certification** |
| 9.5.3.1 | The information provided by the audit team to the certification body for the certification decision shall include, as a minimum: |
| | a) Che audit report; |
| | b) Comments on the nonconformities and, where applicable, the correction and corrective actions |
| | taken by the client; |
| | c) Confirmation of the information provided to the certification body used in the application review (see 9.1.2); |
| | d) Confirmation that the audit objectives have been achieved; |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | e) A recommendation whether or not to grant certification, together with any conditions or observations. |
| 9.5.3.2 | If the certification body is not able to verify the implementation of corrections and corrective actions of any major nonconformity within 6 months after the last day of stage 2, the certification body shall conduct another stage 2 prior to recommending certification. |
| 9.5.3.3 | When a transfer of certification is envisaged from one certification body to another, the accepting certification body shall have a process for obtaining sufficient information in order to take a decision on certification. |
| | NOTE Certification schemes can have specific rules regarding the transfer of certification. |
| **9.5.4** | **Information for granting recertification** |
| | The certification body shall make decisions on renewing certification based on the results of the recertification audit, as well as the results of the review of the system over the period of certification and complaints received from users of certification. |
| **9.6** | **Maintaining certification** |
| **9.6.1** | **General** |
| | The certification body shall maintain certification based on demonstration that the client continues to satisfy the requirements of the management system standard. It may maintain a client's certification based on a positive conclusion by the audit team leader without further independent review and decision, provided that: |
| | a) For any major nonconformity or other situation that may lead to suspension or withdrawal of certification, the certification body has a system that requires the audit team leader to report to the certification body the need to initiate a review by competent personnel (see 7.2.8), different from those who carried out the audit, to determine whether certification can be maintained; |
| | b) Competent personnel of the certification body monitor its surveillance activities, including monitoring the reporting by its auditors, to confirm that the certification activity is operating effectively. |
| **9.6.2** | **Surveillance activities** |
| 9.6.2.1 | **General** |
| IS 9.6.2.1 | **IS 9.6.2 Surveillance activities** |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| 9.6.2.1.1 | The certification body shall develop its surveillance activities so that representative areas and functions covered by the scope of the management system are monitored on a regular basis, and take into account changes to its certified client and its management system. |
| IS 9.6.2.1.1 | Surveillance audit procedures shall be consistent with those concerning the certification audit of the client's ISMS as described in this International Standard. |
| | The purpose of surveillance is to verify that the approved ISMS continues to be implemented, to consider the implications of changes to that system initiated as a result of changes in the client's operation and to confirm continued compliance with certification requirements. Surveillance audit programmes shall cover at least: |
| | a) The system maintenance elements such as information security risk assessment and control maintenance, internal ISMS audit, management review and corrective action; |
| | b) Communications from external parties as required by the ISMS standard IS/ISO/IEC 27001 and other documents required for certification; |
| | c) Changes to the documented system; |
| | d) Areas subject to change; |
| | e) Selected requirements of IS/ISO/IEC 27001; |
| | f) Other selected areas as appropriate |
| CS-L3 | Surveillance audit procedures shall be consistent with those concerning the certification audit of the client's CSMS as described in this International Standard. |
| | The purpose of surveillance is to verify that the approved CSMS continues to be implemented, to consider the implications of changes to that system initiated as a result of changes in the client's operation and to confirm continued compliance with certification requirements. Surveillance audit programmes shall cover at least: |
| | a) The system maintenance elements such as information security risk assessment and control maintenance, internal CSMS audit, management review and corrective action; |
| | b) Communications from external parties as required by the CSMS standard ATC (Level 3) and other documents required for certification; |
| | e) Selected requirements of ATC (Level 3); |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| 9.6.2.1.2 | Surveillance activities shall include on-site auditing of the certified client's management system's fulfilment of specified requirements with respect to the standard to which the certification is granted. Other surveillance activities may include: |
| | a) Enquiries from the certification body to the certified client on aspects of certification; |
| | b) Reviewing any certified client's statements with respect to its operations (e.g. promotional material, website); |
| | c) Requests to the certified client to provide documented information (on paper or electronic media); |
| | d) Other means of monitoring the certified client's performance. |
| IS 9.6.2.1.2 | As a minimum, every surveillance by the certification body shall review the following: |
| | a) The effectiveness of the ISMS with regard to achieving the objectives of the client's information security policy; |
| | b) The functioning of procedures for the periodic evaluation and review of compliance with relevant information security legislation and regulations; |
| | c) Changes to the controls determined, and resulting changes to the SoA; |
| | d) Implementation and effectiveness of controls according to the audit programme |
| CS-L3 | As a minimum, every surveillance by the certification body shall review the following: |
| | a) The effectiveness of the CSMS with regard to achieving the objectives of the client's information security policy; |
| IS 9.6.2.1.3 | The certification body shall be able to adapt its surveillance programme to the information security issues related to risks and impacts on the client and justify this programme. |
| | Surveillance audits may be combined with audits of other management systems. The reporting shall clearly indicate the aspects relevant to each management system. |
| | During surveillance audits, certification bodies shall check the records of appeals and complaints brought before the certification body and, where any nonconformity or failure to meet the requirements of certification is revealed, that the client has investigated its own ISMS and procedures and taken appropriate corrective action. |
| | CS-L3: During surveillance audits, certification bodies shall check the records of appeals and complaints brought before the certification body and, where any nonconformity or |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | failure to meet the requirements of certification is revealed, that the client has investigated its own CSMS and procedures and taken appropriate corrective action. |
| | A surveillance report shall contain, in particular, information on clearing of nonconformities revealed previously and the version of the SoA and important changes from the previous audit. As a minimum, the reports arising from surveillance shall build up to cover in totality the requirements of 9.6.2.1.1 and 9.6.2.1.2 above. |
| 9.6.2.2 | **Surveillance audit** |
| | Surveillance audits are on-site audits, but are not necessarily full system audits, and shall be planned together with the other surveillance activities so that the certification body can maintain confidence that the client's certified management system continues to fulfil requirements between recertification audits. Each surveillance for the relevant management system standard shall include: |
| | a) Internal audits and management review; |
| | b) A review of actions taken on nonconformities identified during the previous audit; |
| | c) Complaints handling; |
| | d) Effectiveness of the management system with regard to achieving the certified client's objectives and the intended results of the respective management system (s); |
| | e) Progress of planned activities aimed at continual improvement; |
| | f) Continuing operational control; |
| | g) Review of any changes; |
| | h) Use of marks and/or any other reference to certification. |
| **9.6.3** | **Recertification** |
| CS-L3 | The condition of ATC (Level 3) is that the CSEs are certified as per BTC (Level 1) and STC (Level 2). In case, at the time of recertification of ATC (Level 3), the validity of either BTC (Level 1) or STC (Level 2) or both are expired then ATC (Level 3) recertification can't be processed. |
| **9.6.3.1** | **Recertification audit planning** |
| IS 9.6.3.1 | **IS 9.6.3 Re-certification audits** |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | Re-certification audit procedures shall be consistent with those concerning the initial certification audit of the client's ISMS as described in this International Standard. |
| | CS-L3: Re-certification audit procedures shall be consistent with those concerning the initial certification audit of the client's CSMS. |
| | The time allowed to implement corrective action shall be consistent with the severity of the nonconformity and the associated information security risk. |
| 9.6.3.1.1 | The purpose of the recertification audit is to confirm the continued conformity and effectiveness of the management system as a whole, and its continued relevance and applicability for the scope of certification. A recertification audit shall be planned and conducted to evaluate the continued fulfilment of all of the requirements of the relevant management system standard or other normative document. This shall be planned and conducted in due time to enable for timely renewal before the certificate expiry date. |
| 9.6.3.1.2 | The recertification activity shall include the review of previous surveillance audit reports and consider the performance of the management system over the most recent certification cycle. |
| 9.6.3.1.3 | Recertification audit activities may need to have a stage 1 in situations where there have been significant changes to the management system, the organization, or the context in which the management system is operating (e.g. changes to legislation). |
| | NOTE Such changes can occur at any time during the certification cycle and the certification body might need to perform a special audit (see 9.6.4), which might or might not be a two-stage audit. |
| **9.6.3.2** | **Recertification audit** |
| 9.6.3.2.1 | The recertification audit shall include an on-site audit that addresses the following: |
| | a) The effectiveness of the management system in its entirety in the light of internal and external changes and its continued relevance and applicability to the scope of certification; |
| | b) Demonstrated commitment to maintain the effectiveness and improvement of the management system in order to enhance overall performance; |
| | c) The effectiveness of the management system with regard to achieving the certified client's objectives and the intended results of the respective management system (s). |
| 9.6.3.2.2 | For any major nonconformity, the certification body shall define time limits for correction and corrective actions. These actions shall be implemented and verified prior to the expiration of certification. |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| 9.6.3.2.3 | When recertification activities are successfully completed prior to the expiry date of the existing certification, the expiry date of the new certification can be based on the expiry date of the existing certification. The issue date on a new certificate shall be on or after the recertification decision. |
| 9.6.3.2.4 | If the certification body has not completed the recertification audit or the certification body is unable to verify the implementation of corrections and corrective actions for any major nonconformity (see 9.5.2.1) prior to the expiry date of the certification, then recertification shall not be recommended and the validity of the certification shall not be extended. The client shall be informed and the consequences shall be explained. |
| 9.6.3.2.5 | The Following expiration of certification, the certification body can restore certification within 6 months provided that the outstanding recertification activities are completed, otherwise at least a stage 2 shall be conducted. The effective date on the certificate shall be on or after the recertification decision and the expiry date shall be based on prior certification cycle. |
| **9.6.4** | **Special audits** |
| 9.6.4.1 | **Expanding scope** |
| | The certification body shall, in response to an application for expanding the scope of a certification already granted, undertake a review of the application and determine any audit activities necessary to decide whether or not the extension may be granted. This may be conducted in conjunction with a surveillance audit. |
| IS 9.6.4.1 | **IS 9.6.4 Special cases** |
| | The activities necessary to perform special audits shall be subject to special provision if a client with a certified ISMS makes major modifications to its system or if other changes take place which could affect the basis of its certification |
| CS-L3 | **IS 9.6.4 Special cases** |
| | The activities necessary to perform special audits shall be subject to special provision if a client with a certified CSMS makes major modifications to its system or if other changes take place which could affect the basis of its certification |
| 9.6.4.2 | **Short-notice audits** |
| | It may be necessary for the certification body to conduct audits of certified clients at short notice or unannounced to investigate complaints, or in response to changes, or as follow up on suspended clients. In such cases: |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | a) The certification body shall describe and make known in advance to the certified clients (e.g. in |
| | documents as described in 8.5.1) the conditions under which such audits will be conducted; |
| | b) The certification body shall exercise additional care in the assignment of the audit team because of the lack of opportunity for the client to object to audit team members. |
| **9.6.5** | **Suspending, withdrawing or reducing the scope of certification** |
| 9.6.5.1 | The certification body shall have a policy and documented procedure(s) for suspension, withdrawal or reduction of the scope of certification, and shall specify the subsequent actions by the certification body. |
| 9.6.5.2 | The certification body shall suspend certification in cases when, for example: |
| | —the client's certified management system has persistently or seriously failed to meet certification requirements, including requirements for the effectiveness of the management system; |
| | —the certified client does not allow surveillance or recertification audits to be conducted at the required frequencies; |
| | —the certified client has voluntarily requested a suspension. |
| 9.6.5.3 | Under suspension, the client's management system certification is temporarily invalid. |
| 9.6.5.4 | The certification body shall restore the suspended certification if the issue that has resulted in the suspension has been resolved. Failure to resolve the issues that have resulted in the suspension in a time established by the certification body shall result in withdrawal or reduction of the scope of certification. |
| | **Note** In most cases, the suspension would not exceed six months. |
| 9.6.5.5 | The certification body shall reduce the scope of certification to exclude the parts not meeting the requirements, when the certified client has persistently or seriously failed to meet the certification requirements for those parts of the scope of certification. Any such reduction shall be in line with the requirements of the standard used for certification. |
| **9.7** | **Appeals** |
| 9.7.1 | The certification body shall have a documented process to receive, evaluate and make decisions on appeals. |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| 9.7.2 | The certification body shall be responsible for all decisions at all levels of the appeals-handling process. The certification body shall ensure that the persons engaged in the appeals-handling process are different from those who carried out the audits and made the certification decisions. |
| 9.7.3 | Submission, investigation and decision on appeals shall not result in any discriminatory actions against the appellant. |
| 9.7.4 | The appeals-handling process shall include at least the following elements and methods: |
| | a) An outline of the process for receiving, validating and investigating the appeal, and for deciding what |
| | actions need to be taken in response to it, taking into account the results of previous similar appeals; |
| | b) Tracking and recording appeals, including actions undertaken to resolve them; |
| | c) Ensuring that any appropriate correction and corrective action are taken. |
| 9.7.5 | The certification body receiving the appeal shall be responsible for gathering and verifying all necessary information to validate the appeal. |
| 9.7.6 | The certification body shall acknowledge receipt of the appeal and shall provide the appellant with progress reports and the result of the appeal. |
| 9.7.7 | The decision to be communicated to the appellant shall be made by, or reviewed and approved by, individual(s) not previously involved in the subject of the appeal. |
| 9.7.8 | The certification body shall give formal notice to the appellant of the end of the appeals-handling process. |
| **9.8** | **Complaints** |
| 9.8.1 | The certification body shall be responsible for all decisions at all levels of the complaints-handling process. |
| 9.8.2 | Submission, investigation and decision on complaints shall not result in any discriminatory actions against the complainant. |
| 9.8.3 | Upon receipt of a complaint, the certification body shall confirm whether the complaint relates to certification activities that it is responsible for and, if so, shall deal with it. If the complaint relates to a certified client, then examination of the complaint shall consider the effectiveness of the certified management system. |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| 9.8.4 | Any valid complaint about a certified client shall also be referred by the certification body to the certified client in question at an appropriate time. |
| 9.8.5 | The certification body shall have a documented process to receive, evaluate and make decisions on complaints. This process shall be subject to requirements for confidentiality, as it relates to the complainant and to the subject of the complaint. |
| 9.8.6 | The complaints-handling process shall include at least the following elements and methods: |
| | a) An outline of the process for receiving, validating, investigating the complaint, and for deciding |
| | what actions need to be taken in response to it; |
| | b) racking and recording complaints, including actions undertaken in response to them; |
| | c) Ensuring that any appropriate correction and corrective action are taken. |
| | **Note** ISO 10002 provides guidance for complaints handling. |
| 9.8.7 | The certification body receiving the complaint shall be responsible for gathering and verifying all necessary information to validate the complaint. |
| 9.8.8 | Whenever possible, the certification body shall acknowledge receipt of the complaint, and shall provide the complainant with progress reports and the result of the complaint. |
| 9.8.9 | The decision to be communicated to the complainant shall be made by, or reviewed and approved by, individual(s) not previously involved in the subject of the complaint. |
| 9.8.10 | Whenever possible, the certification body shall give formal notice of the end of the complaints-handling process to the complainant. |
| 9.8.11 | The certification body shall determine, together with the certified client and the complainant, whether and, if so to what extent, the subject of the complaint and its resolution shall be made public. |
| **9.9** | **Client records** |
| 9.9.1 | The certification body shall maintain records on the audit and other certification activities for all clients, including all organizations that submitted applications, and all organizations audited, certified, or with certification suspended or withdrawn. |
| 9.9.2 | Records on certified clients shall include the following: |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | a) Application information and initial, surveillance and recertification audit reports; |
| | b) Certification agreement; |
| | c) Justification of the methodology used for sampling of sites, as appropriate; |
| | **Note** Methodology of sampling includes the sampling employed to audit the specific management system and/or to select sites in the context of multi-site audit. |
| | d) Justification for auditor time determination (see 9.1.4); |
| | e) Verification of correction and corrective actions; |
| | f) Records of complaints and appeals, and any subsequent correction or corrective actions; |
| | g) Committee deliberations and decisions, if applicable; |
| | h) Documentation of the certification decisions; |
| | i) Certification documents, including the scope of certification with respect to product, process or service, as applicable; |
| | j) Related records necessary to establish the credibility of the certification, such as evidence of the competence of auditors and technical experts; |
| | k) Audit programmes. |
| 9.9.3 | he certification body shall keep the records on applicants and clients secure to ensure that the information is kept confidential. Records shall be transported, transmitted or transferred in a way that ensures that confidentiality is maintained. |
| 9.9.4 | The certification body shall have a documented policy and documented procedures on the retention of records. Records of certified clients and previously certified clients shall be retained for the duration of the current cycle plus one full certification cycle. |
| | **Note** In some jurisdictions, the law stipulates that records need to be maintained for a longer time period. |
| **10** | **Management system requirements for certification bodies** |
| **10.1** | **Options** |
| | The certification body shall establish, document, implement and maintain a management system that is capable of supporting and demonstrating the consistent |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | achievement of the requirements of this part of IS/ISO/IEC 17021. In addition to meeting the requirements of Clauses 5 to 9, the certification body shall implement a management system in accordance with either: |
| | a) General management system requirements (see 10.2); or |
| | b) Management system requirements in accordance with ISO 9001 (see 10.3). |
| **10.2** | **Option A: General management system requirements** |
| 10.2.1 | **General** |
| | The certification body shall establish, document, implement and maintain a management system that is capable of supporting and demonstrating the consistent achievement of the requirements of this part of IS/ISO/IEC 17021. |
| | The certification body's top management shall establish and document policies and objectives for its activities. The top management shall provide evidence of its commitment to the development and implementation of the management system in accordance with the requirements of this part of IS/ISO/IEC 17021. The top management shall ensure that the policies are understood, implemented and maintained at all levels of the certification body's organization. |
| | The certification body's top management shall assign responsibility and authority for: |
| | a) Ensuring that processes and procedures needed for the management system are established, implemented and maintained; |
| | b) Reporting to top management on the performance of the management system and any need for improvement. |
| 10.2.2 | **Management system manual** |
| | All applicable requirements of this part of IS/ISO/IEC 17021 shall be addressed either in a manual or in associated documents. The certification body shall ensure that the manual and relevant associated documents are accessible to all relevant personnel. |
| 10.2.3 | **Control of documents** |
| | The certification body shall establish procedures to control the documents (internal and external) that relate to the fulfilment of this part of IS/ISO/IEC 17021. The procedures shall define the controls needed to: |
| | a) Approve documents for adequacy prior to issue; |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | b) Review and update where necessary and re-approve documents; |
| | c) Ensure that changes and the current revision status of documents are identified; |
| | d) Ensure that relevant versions of applicable documents are available at points of use; |
| | e) Ensure that documents remain legible and readily identifiable; |
| | f) Ensure that documents of external origin are identified and their distribution controlled; |
| | g) Prevent the unintended use of obsolete documents, and to apply suitable identification to them if they are retained for any purpose. |
| | NOTE Documentation can be in any form or type of medium. |
| 10.2.4 | The certification body shall establish procedures to define the controls needed for the identification, storage, protection, retrieval, retention time and disposition of its records related to the fulfilment of this part of IS/ISO/IEC 17021. |
| | The certification body shall establish procedures for retaining records for a period consistent with its contractual and legal obligations. Access to these records shall be consistent with the confidentiality arrangements. |
| | **Note** For requirements for records on certified clients, see also 9.9. |
| **10.2.5** | **Management review** |
| 10.2.5.1 | **General** |
| | The certification body's top management shall establish procedures to review its management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness, including the stated policies and objectives related to the fulfilment of this part of IS/ISO/IEC 17021. These reviews shall be conducted at least once a year. |
| 10.2.5.2 | **Review inputs** |
| | The input to the management review shall include information related to: |
| | a) Results of internal and external audits; |
| | b) Feedback from clients and interested parties; |
| | c) Safeguarding impartiality; |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | d) The status of corrective actions; |
| | e) The status of actions to address risks; |
| | f) Follow-up actions from previous management reviews; |
| | g) The fulfilment of objectives; |
| | h) Changes that could affect the management system; |
| | i) Appeals and complaints. |
| 10.2.5.3 | **Review outputs** |
| | The outputs from the management review shall include decisions and actions related to |
| | a) Improvement of the effectiveness of the management system and its processes; |
| | b) Improvement of the certification services related to the fulfilment of this part of IS/ISO/IEC 17021; |
| | c) Resource needs; |
| | d) Revisions of the organization's policy and objectives. |
| **10.2.6** | **Internal audits** |
| 10.2.6.1 | The certification body shall establish procedures for internal audits to verify that it fulfils the requirements of this part of IS/ISO/IEC 17021 and that the management system is effectively implemented and maintained. |
| | **Note** ISO 19011 provides guidelines for conducting internal audits. |
| 10.2.6.2 | An audit programme shall be planned, taking into consideration the importance of the processes and areas to be audited, as well as the results of previous audits. |
| 10.2.6.3 | Internal audits shall be performed at least once every 12 months. The frequency of internal audits may be reduced if the certification body can demonstrate that its management system continues to be effectively implemented according to this part of IS/ISO/IEC 17021 and has proven stability. |
| 10.2.6.4 | The certification body shall ensure that: |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | a) Internal audits are conducted by competent personnel knowledgeable in certification, auditing and the requirements of this part of IS/ISO/IEC 17021; |
| | b) Auditors do not audit their own work; |
| | c) Personnel responsible for the area audited are informed of the outcome of the audit; |
| | d) Any actions resulting from internal audits are taken in a timely and appropriate manner; |
| | e) Any opportunities for improvement are identified. |
| **10.2.7** | **Corrective actions** |
| | The certification body shall establish procedures for identification and management of nonconformities in its operations. The certification body shall also, where necessary, take actions to eliminate the causes of nonconformities in order to prevent recurrence. Corrective actions shall be appropriate to the impact of the problems encountered. The procedures shall define requirements for: |
| | a) Identifying nonconformities (e.g. from valid complaints and internal audits); |
| | b) Determining the causes of nonconformity; |
| | c) Correcting nonconformities; |
| | d) Evaluating the need for actions to ensure that nonconformities do not recur; |
| | e) Determining and implementing in a timely manner, the actions needed; |
| | f) Recording the results of actions taken; |
| | g) Reviewing the effectiveness of corrective actions. |
| **10.3** | **Option B: Management system requirements in accordance with ISO 9001** |
| 10.3.1 | **General** |
| | The certification body shall establish and maintain a management system, in accordance with the requirements of ISO 9001, which is capable of supporting and demonstrating the consistent achievement of the requirements of this part of IS/ISO/IEC 17021, amplified by 10.3.2 to 10.3.4. |
| 10.3.2 | **Scope** |

| CLAUSE No. of IS/ISO/IEC 17021-1: 2015 and IS/ISO/IEC 27006:2015 | DESCRIPTION |
|---|---|
| | For application of the requirements of ISO 9001, the scope of the management system shall include the design and development requirements for its certification services. |
| 10.3.3 | **Customer focus** |
| | For application of the requirements of ISO 9001, when developing its management system, the certification body shall consider the credibility of certification and shall address the needs of all parties (as set out in 4.1.2) that rely upon its audit and certification services, not just its clients. |
| 10.3.4 | **Management review** |
| | For application of the requirements of ISO 9001, the certification body shall include as input for management review, information on relevant appeals and complaints from users of certification activities and a review of impartiality. |

**Annexure B**

**Competence of Certification Functions for Additional Technical Criteria (Level 3)**

Educational qualifications and experience of the certification functions of CBs of CSMS for ATC (Level 3) is described below:

| S No. | Role | Education | Competency Knowledge and Skills | Experience | Training Requirements |
|---|---|---|---|---|---|
| 1 | Head – Certification Body | As per organisation policy | To manage certification scheme | 20 years in management position | Acquired knowledge of conformity assessment system including auditing, requirements covered in CSMS scheme for ATC (Level 3). |
| 2 | Audit Team Leader (CSMS Lead Auditor- ATC (Level 3)) | Graduate in computer science, computer engineering, telecommunication engineering, cyber security, electronics and information technology, instrumentation and control, software engineering, information systems etc. | As per Note 2 of this annexure. | a. 10 audits with 2 as a TL {can be ISMS and/or CSMS (BTC (Level 1),STC (Level 2) ,ATC (Level 3)) of various organisations.<br><br>b. Industrial work experience (in ICS) – 2 years<br><br>c. Total experience (in ICS and IT) – 6 years in cyber security | a. Should have undergone IS/ISO/IEC 27001:2022 Lead Auditor course and requirements of BTC (Level 1), STC (Level 2) and ATC (Level 3)<br><br>b. 24 hours training in Cyber Security issues, rationale of controls in Level 3 and their auditing techniques as per Note 1.<br><br>Note : Refer to Note 1, 2 and 3 of this annexure. |

| S No. | Role | Education | Competency Knowledge and Skills | Experience | Training Requirements |
|---|---|---|---|---|---|
| 3 | CSMS Auditors (ATC Level 3)) | As mentioned above | As mentioned above | a. 10 audits (can be ISMS and/or CSMS (Level 1, 2 ,3) audits)<br><br>b. Total industrial work experience (in ICS) – 3 years<br><br>c. Total experience (in ICS and IT) – 6 years in cyber security of ICS | As per Note 1, 2 and 3 of this annexure |
| 4 | Technical Experts | As mentioned above | Knowledge on rationale of requirements of IEC 62443 family of standards and ICS technologies | 10 years of experience in academic institute/ICS industry/freelance consultancy in the area of Power/Energy sector and knowledge acquisition as per Note 2. | Formal training on overview of BTC (Level 1), STC (Level 2) and ATC (Level 3) and Certification Process (8 hours)<br><br>Should possess Knowledge and Skill modules of the certifications mentioned in Note 3 |
| 5 | CB Secretariat | Graduate | Knowledge of ATC (Level 3) and Certification Process | 3 years of experience in operating conformity assessment schemes | Formal training on ATC (Level 3) and Certification Process (24 hours) |

Note 1: Trainings acquired (minimum 40 hours) by auditors working in a CB is described below:

a. The technology used for the manufacture of the products/infrastructure audited, the operation of processes and the delivery of services, Level 3 criteria.
b. The way in which products/components are used, processes are operated, and services are delivered; review of compensating countermeasures, concept of zone and conduit security, levels, etc.

Note 2: Training on modules configuring the following certifications (refer to Scheme for PrCB) focusing on IEC 62443-2-1, IEC 62443-2-3, IEC 62443-3-2 and IEC 62443-3-3:

i. ICS Cyber Risk Assessment (Advanced)
ii. ICS Cyber Security Design & Implementation (Advanced)
iii. ICS Cyber Security Operations & Maintenance (Advanced)

Note 3: Training on modules configuring the following certifications:

i. ICR-A ICS Cyber Risk Assessment (Advanced)
ii. ICD-A ICS Cyber Security Design & Implementation (Advanced)
iii. CD-M ICS Cyber Security Design & Implementation (Master)
iv. ICM-A ICS Cyber Security Operations & Maintenance (Advanced)

Note 4: The ATC (Level 3) training requirements are in addition to STC (Level 2).

**SECTION 6**

# PROVISIONAL APPROVAL SYSTEM

## 1. Introduction

1.1. To operate certification Scheme of CSMS, as per ATC (Level 3), for CSEs, the certification body (CB) shall need to primarily comply with the requirements specified in **certification body requirements** defined in Section 5 of this document for obtaining accreditation from NABCB.

1.2. For demonstrating compliance with the **certification body requirements,** CBs are required to demonstrate that they have an experience of auditing minimum 2 clients (CSEs) as per this ATC (Level 3). There may be a situation where CB may not get a client for audit and certification, since in the beginning to get accreditation, they have to demonstrate their experience of audit and certification to the accreditation body and at the same time the client (CSEs) may not be willing to have a contract with unaccredited certification bodies. As a result, CB may not be able to approach accreditation body (NABCB / or any other AB which is signatory of IAF ) to get initial accreditation or to get the relevant accreditation scope extension, if already accredited. To address this situation, it is necessary to have a mechanism in place without any compromise on the technical criteria and competence of personnel (auditors / experts) so that confidence of the users on the system is maintained.

1.3. Further, in order to launch the Scheme, it is necessary that some CBs are available at the beginning.

1.4. Therefore, it is necessary to establish a procedure for provisional approval of CBs under the Scheme till such time they can get formally accredited so that an initiation of process between CBs an CSEs can be facilitated.

1.5. This document sets out the requirements for provisional approval, to be fulfilled by CBs desirous of operating under the Scheme pending formal accreditation.

1.6. In order to be formally accredited by the NABCB **/** or any other AB which is signatory of IAF , the CB, would need to undergo a short Office Assessment including a Witness Assessment of an actual evaluation under the Scheme.

## 2. Purpose

2.1. This document defines the procedure and requirements for provisional approval for Certification Bodies, operating under the scheme, pending formal accreditation. This procedure is required primarily to facilitate the MSMEs, Start Ups, Stand Up India entrepreneurs so that they can join the ecosystem as a potential CB.

## 3. Scope

3.1. This document defines the procedure for CBs to obtain provisional approval to operate under the Scheme for Conformity Assessment Framework for CSEs, pending formal accreditation by the NABCB / any other IAF member accreditation body as per the prescribed requirements.

3.2. This approval shall be valid for a period of one year within which the provisionally approved CB would have to obtain formal NABCB / any other IAF member accreditation body accreditation.

3.3. This scope covers the certification requirements as per the ATC (Level 3).

## 4. Objective

The objectives of provisional approval are to:

4.1. Provide a mechanism of provisional approval to CB to ensure its certification processes get stabilised and get accredited.

4.2. Demonstration of competencies by CB.

## 5. Requirement for Provisional Approval

The Certification Bodies desirous of providing certification services to clients and intended to get accreditation within a period of one year shall meet the requirements as prescribed below in this document.

### 5.1 Administrative Requirements

#### 5.1.1 Legal Entity

The CB shall be a legal entity or shall be a defined part of a legal entity, such that it can be held legally responsible for all its certification activities. A governmental CB is deemed to be a legal entity on the basis of its governmental status. A CB, that is part of an organization involved in functions other than certification, shall be separate and identifiable within that organization.

#### 5.1.2 Organisational Structure

The CB shall define and document the duties, responsibilities and reporting structure of its personnel and any committee and its place within the organisation. When the CB is a defined part of a legal entity, documentation of the organisational structure shall include the line of authority and the relationship to other parts within the same legal entity. The permanent / regular minimum resource strength in terms of professionals in CBs shall not be less than two (including 1 auditor and 1 technical reviewer)

### 5.2 Criteria

The potential CB shall be fully aware about the requirements of certification and provisional approval including technical criteria and an applicable procedure as defined in the framework. They should abide by the requirements pertaining to Impartiality and Independency.

There could be following scenarios:

5.2.1. CB doesn't possess any experience of certification but have the technical competence. They have a commitment to establish a CB for the applied scope.

5.2.2. CB is established but doesn't operate in the sector of IT (IAF code 33). Presently engaged in QMS and EMS certification. They have built the technical competence

and resources in IT/ ISMS/ CSMS in recent times and formalizing the established processes.

5.2.3. CB operate in the IT sector (e.g. QMS) and intend to expand for ISMS and CSMS. In recent times, they have established the processes for the same.
For all the three scenarios, the CBs shall meet the technical criteria defined in this document, however they can conduct common audit if the CSE has opted for integrated management system.

**5.3 The certification body shall meet the following eligibility requirements**

5.3.1. Undertaking to comply with the criteria of accreditation within one year along with plan of activities and roadmap for compliance. (with NABCB / any other IAF accreditation member)

5.3.2. The CB shall have at least two ISO 27001 lead auditors (refer to Annex A of this Section for resource requirements) having minimum five-year relevant industry experience or with minimum 20 no. of man-days audit experience in ISO 27001 certification.

5.3.3. Acquired complete understanding of the ATC (Level 3).

5.3.4. Shall have implemented the requirements of QMS (refer to Annex A of this Section).

5.3.5. Until the period, the entity is under provisional approval or a period of 1 year whichever is earlier, the QCI may relax the competency requirements commensurating to the scope applied.

5.1 **Integrity**

The CB and its personnel shall maintain integrity at all times. The CB shall implement adequate measures to ensure integrity by facilitating police verification and background check.

5.2 **Impartiality**

5.2.1 The CB shall be impartial.

5.2.2 The CB shall be so structured and managed as to safeguard impartiality.

5.2.3 The CB and its staff shall not engage in any activities that may conflict with their Impartiality.

5.2.4 The CB shall act impartially in relation to its applicants, candidates and certified CSEs.

The CB shall have a process to identify, analyse, evaluate, monitor, and document the threats to impartiality arising from its activities including any conflicts arising from its relationships on an ongoing basis.

This shall include those threats that may arise from its activities, or from its relationships, or from the relationships of its personnel. Where there are any threats to impartiality, the CB 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 CB or from the activities of other persons, bodies or organizations.

a. Top management shall review any residual risk to determine if it is within the level of acceptable risk. When a relationship poses an unacceptable threat to impartiality, then certification shall not be provided.

b. The risk assessment process shall include identification of and consultation with appropriate interested parties to advice on matters affecting impartiality including openness and public perception.

NOTE 1: Sources of threats to impartiality of the accreditation body 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.

5.2.5 The CB shall not impart education and/or training in Cyber Security domain within the same legal entity.

5.2.6 The CB shall have a process to eliminate or minimize risk to impartiality if training/ education of CSEs is carried out in a related body which is linked to the CB by common ownership etc.

5.2.7 The CB shall have a process to ensure that the auditors / experts are free of any conflict of interest with the applicant(s) by means of being a consultant for applicant in the past.

5.3 **Confidentiality**

The CB shall ensure confidentiality of information obtained in the course of its certification activities by having a suitable system. Information gathered would not be used for any commercial or other purposes other than that to support certification of CSEs.

5.4 **Safety and Security**

The CB shall develop and document policies and procedures to ensure safety and security throughout the certification process.

## 6. Certification process

6.1 The CB shall manage the process of certifying CSEs as per the documented ‘Certification Process for CBs’ prescribed under the Scheme.

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

6.3 The CB shall ensure the requirements of the Scheme are met with at any point in time.

6.4 The CB shall certify CSEs only under the Scheme and shall use the logo of the Scheme in the certificates issued to the certified CSEs.

6.5 The CB shall have written agreement with the certified CSEs on the use of the certificate issued to them.

6.6 The CB shall have a process to handle appeals by the candidates against any of its decisions.

6.7 The CB shall have a process to handle complaints from the CSEs, the users of the services of the certified CSEs or any other stake holder.

6.8 **Certification agreement**

The CBs shall have a legally enforceable agreement for the provision of certification activities to CSEs. In addition, the CBs shall ensure its certification agreement requires that the CSEs comply at least, with the specific requirements as prescribed in the relevant accreditation standards (IS/ISO/IEC 17021 -1) and the Scheme document.

The certification agreement shall include the mechanism to handle certified clients if CB does not extend approval or withdraws from accreditation.

6.9 **Responsibility for decision on certification**

The CBs shall be responsible for, shall retain authority for, and shall not delegate, its decisions relating to certification, including the granting, maintaining, recertifying, expanding and reducing the scope of the certification, and suspending or withdrawing the certification.

6.10 **Publicly available information**

6.10.1 The CB shall maintain a website for providing information about the Scheme and its certification activities under the Scheme.

6.10.2 The CB shall maintain and make publicly available 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.

6.10.3 The CB shall make publicly available information about applications registered and certifications granted, suspended or withdrawn.

6.10.4 The CB shall make publicly available its process for handling appeals and complaints.

## 7. Approval Process

### Application

7.1 Any organization interested in approval as a CB for the purpose of the 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.

7.2 The filled in application form for approval shall be duly signed by the HoD/authorized representative/s of the organization seeking approval.

7.3 On receipt of the application form, it will be scrutinized by the QCI and those found complete in all respects will be processed further.

## 8. Assessment Process

8.1 Interested CB shall apply in the prescribe application form to the QCI for seeking provisional approval.

8.1.1 If an applicant CB is already QCI accredited for ISMS/CSMS for BTC (Level 1) and STC (Level 2) certification, then they shall submit their procedure for auditing for the requirements specified in ATC (Level 3).

8.1.2 They shall have trained their auditors on technical aspects of the requirements of ATC (Level 3) with desired competency.

If QCI is satisfied with these two requirements, then there will not be any on-site audit.

8.2 Upon review of the application for completeness by QCI, an assessment team comprising a team leader and member(s) / technical expert(s) will be nominated for the purpose of assessment at applicant's office and other locations, if required. The duration of assessment for document review and on-site assessment shall be applicable as per defined man-day and fee structure.

8.3 The names of the members of the assessment team along with their CVs will be communicated to the applicant CB 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 undertakings regarding confidentiality and conflict of interest.

8.4 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 accreditation process by the applicant.

8.5 The assessment team leader shall provide an assessment plan to the applicant CB in advance of the assessment.

8.6 The date(s) of assessment shall be mutually agreed upon between the applicant CB and QCI assessment team.

8.7 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 organisation 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 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.

8.8 At the end of the Office Assessment, through a formal closing meeting, all the nonconformities 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.

8.9 Based on the report of assessment, and the action taken by the applicant on the nonconformities/ concerns, if any, QCI shall take a decision on whether to; a) Undertake Witness Assessments(s) (WA) of actual evaluation or any part of the accreditation process by the applicant prior to granting of provisional approval or, b) Granting provisional approval to the applicant as accreditation body under the Scheme.

8.10 AB may conduct Knowledge and Skill tests of auditor(s) and technical expert(s) as deemed fit.

## 9. Validity of Provisional Approval

9.1 The approval shall be valid for a period of one year.

9.2 During the validity of approval, QCI shall undertake at least one Witness Assessment to confirm the CB's competence.

9.3 The CB shall obtain formal accreditation as per the Accreditation Scheme for CBs for operating CSMS within one year of provisional approval by QCI.

9.4 Based on the request of the CB and review of previous performance, it may be decided to extend the period of validity; in such a case, the CB shall be assessed covering both office and witnessing on-site, as decided by QCI, prior to such an extension. Extension of validity should not be more than 6 months.

9.5 The provisional 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.

9.6 The approved CB shall inform QCI without delay about any changes relevant to its provisional approval, in any aspect of its status or operation relating to;

9.6.1 Its legal, commercial, ownership or organizational status,
9.6.2 The organisation, top management and key personnel,
9.6.3 Main policies, resources, premises and scope of approval, and
9.6.4 Other such matters that may affect the ability of the CB to fulfil the requirements for approval.

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

## 10. Fee

The CB shall abide by the commercials as applicable.

**Annexure A**

## A. Requirements for developing CBs' Quality Assurance System (CB-QAS)

Certification Bodies should have quality assurance system for continually improving the delivery and effectiveness of Cybersecurity certification services. It could be based on Quality Management System (QMS) principles, however CB-QAS of the organization shall have the procedures prescribed below, as minimum:

i. Procedure for reviewing and evaluating applicants' documents pertaining to CSMS system including the risk management
ii. Procedure for selecting and monitoring expert / auditor for the Cybersecurity Certification
iii. Procedure for management of audit activities
iv. Procedure for decision making (i.e. granting, maintaining suspension, withdrawal etc.)
v. Procedure for Internal Audit and Management Review.

Note: If organisations has implemented ISO 9001 standard, the above requirements are deemed compliant.

## B. Resource and Competence Requirements

The applicant CB shall have a procedure to ensure that auditors are trained in the following areas and competent to carry out the audit as per the requirements of ATC (Level 3) (Refer to Annex B in Section 5 of this document).

**SECTION 7**

# RULES FOR USE OF SCHEME MARK

## 1. Introduction

1.1 The certification scheme for Certification Bodies is designed and developed as per international best practices.

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

1.3 The Mark is allowed to be used for promotion by accredited CBs, who are allowed to display the mark as per the prescribed rules mentioned in the subsequent paras of this document.

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

## 2. Purpose

The QCI and its constituent accredited organisations can benefit from visually identifying their status through the use of the Scheme Mark. In doing so, the Mark Holders are provided guidance in a manner that organisations displaying the Mark shall desist from misleading anyone; avoid positioning of incompatible marks that may devalue or degrade other Marks; use them illegally (they are protected trademarks); or use them contrary to the recognised Scheme.

## 3. Objective

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

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

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

## 4. Scope

4.1 The scope covers all the authorized Mark Holders.

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

## 5. Prerequisites for Use of Scheme Mark

### 5.1 Organisations as Entities

5.1.1. The Mark holders that have been approved under the Scheme, are eligible to use Scheme Mark. They are required to submit an application authorising them for Use of Scheme Mark (refer to Annex A of this Section).

5.1.2. As per the contract between the Scheme Manager (QCI) and the mark holder, the mark holder shall be required to formally sign an agreement with QCI for the use of Scheme

Mark. This shall be done immediately after the grant of approval.

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

## 6. Oversight Responsibility

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

6.2 The Mark Holder should have a strong market surveillance system to ensure that compliance 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 needs to comply with applicable criteria in totality.

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

7.3 The mark may also be used by the accredited CBs for their promotion. However, they are not allowed to use the same while issuing consulting documents to their clients.

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

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

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

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

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

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

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

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

7.12 If a Mark holder's accreditation is suspended; its attestation cancelled, withdrawn or discontinued, it is the Mark holder's responsibility to discontinue the use of the Scheme Mark from the date from which the certificate stands suspended, cancelled, and withdrawn or discontinuation comes into force. QCI, the Scheme Manager, that has approved the use of Scheme Mark to the Mark holder, needs to ensure compliance as stated above.

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

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

7.15 Misuse scenarios

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

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

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

## 8. Conditions for use of Scheme Mark by Mark Holder Organisations (CBs)

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

## 9. Conditions for Use of the Scheme Mark by CBs

9.1 The Scheme Mark will be displayed only on the certificate issued to the clients of an accredited CB. The client will not use or display the Scheme Mark anywhere else.

9.2 The client shall abide by all clauses as mentioned in Annex B of this Section once certified, committing to the requirement of the Scheme through their CBs.

9.3 The CBs shall forward the filled contract form received from the certified clients to QCI, for the purpose of signing and completing the contract formalities. Along with the contract form, the relevant conformity assessment body shall also forward the details of the Mark holder, covering as a minimum the following information:

9.3.1 Name and address of the Mark holder;
9.3.2 Legal entity Status (with evidence);
9.3.3 Names of the top management/ownership details;
9.3.4 Details of the certification granted – number, validity, etc.;
9.3.5 Scope of certification granted to the Mark holder;
9.3.6 Any other significant detail(s) considered as relevant.

9.4 The client is required to submit an undertaking to the respective accredited CBs for abiding by the rules for use of scheme Mark.

9.5 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.

9.6 The annual fee for use of Scheme Mark from the Mark holder to be submitted to QCI through the CBs.

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

## 10. Design of the Mark

The Scheme Mark below, is only allowed to be used by the accredited CBs while issuing the statement of conformance.


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

GRAY: C-43, M-33, Y-35, K-2

BLACK: C-66, M-65, Y-60, K-56

**Annexure A**

## Format for Application

### APPLICATION FOR PERMISSION TO USE THE SCHEME MARK

| | | |
|---|---|---|
| **1** | **Name of the applicant CB** | |
| **2** | **Address** | |
| **3** | **Telephone No.** | |
| **4** | **Mobile No.** | |
| **5** | **Email** | |
| **6** | **Purpose of Usage** | |
| **7** | **Duration of Usage** | |
| **8** | **Certification scope of CSEs (for which Scheme Mark is to be applied)** | |
| **9** | **Signature and Date** | |

**Annexure B**

**Format for the agreement between QCI and the Mark holder for use of Scheme Mark (Only for CBs)**

**AGREEMENT FOR USE OF SCHEME MARK**

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

**1. GENERAL CONDITIONS**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## 2. OTHER REQUIREMENTS

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

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

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

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

2.5 Dispute, if any, arising out of the terms and conditions of the agreement between QCI and the Mark holder, shall be governed by laws of India and subject to the jurisdiction

of competent courts located in Delhi.

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

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

**1. Signature :**

**Name of Mark holder:** _____

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

**Title :**

**Address :**

_____

**Date :** _____

**2. Quality Council of India**

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

**Authorized Signatory:** _____

**Name :** _____

**Title :** _____

**Date :** _____