NCIIPC – QCI Initiative

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

Issue No. 1 | Feb 2024

Scheme for Inspection of Critical Sector Entities

DISCLAIMER

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

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

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

PREFACE

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

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

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

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

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

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

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

This document is a part of the CAF specific to Inspection Scheme for Critical Sector Entities. Inspection Bodies, hereafter have been referred to as IBs in this document.

ACKNOWLEDGEMENT

The Quality Council of India (QCI) would like to express gratitude to NCIIPC for assigning us the responsibility of developing a conformity assessment framework to enhance cybersecurity in critical sector entities across India.

At the outset, we would like to express our sincere gratitude to Shri Navin Kumar Singh, DG, NCIIPC, for providing us with the opportunity to collaborate on the initiative aimed at securing the cyber security ecosystem. We also extend our appreciation to Shri Lokesh Garg (DDG), NCIIPC and Col. K. Pradeep Bhat (Retd.) (Consultant), NCIIPC, for their valuable contributions to the finalization of the documents. A special mention is deserved for Gp. Capt. (Dr.) R.K. Singh, (Director), NCIIPC, for skillfully steering the project and fostering 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 throughout its course.

We express 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 that have been instrumental in shaping the structure of the Scheme. We would like to acknowledge, with much appreciation, the technical inputs of Shri U.K. Nandwani, former DG, STQC; Shri Anand Bhatnagar, accreditation expert; and Shri Krishnamurthy Srinivasan, conformity assessment expert.

The efforts of Shri Shivesh Sharma, Accreditation Officer at PADD, are duly recognized for his dedication, commitment, and hard work. The document was made possible through the efforts of the team comprising of Ms. Arushi Lohani and Ms. Rakhi Wadhwa 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	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 Company Limited
11	Sh. Ranvijay Bihari	National Accreditation Board for Education and Training
12	Ms. Reena Garg	Bureau of Indian Standards
13	Prof. Sandeep Shukla	IIT-Kanpur
14	Ms. Seema Mittal	National Critical Information Infrastructure Protection Centre
15	Sh. Shaleen Khetarpaul	BSES Rajdhani Ltd.
16	Sh. Sivakumar V	Central Power Research Institute
17	Sh. Sushil Kumar Nehra	Ministry of Electronics and Information Technology
18	Sh. Vasant Prabhu / Sh. Aamir Hussain	Tata Power – DDL
19	Sh. Vinayak Godse	Data Security Council of India

3. Certification Committee

S No.	Name	Organisation
Chair		
1	Dr. N. Rajesh Pillai	Defence Research and Development Organisation
Members		
2	Sh. Ajay Bagati	Bharat Heavy Electricals Ltd.
3	Sh. Anand Deep Gupta	National Accreditation Board for Certification Bodies
4	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 dynamic nature of cyberspace is leading to a complex transition that significantly impacts various fields, including the security of its citizens. This impact is particularly emphasized due to the extensive reliance on IT infrastructure by Critical Sector Entities (CSEs). This dependency underscores the necessity for a framework that instils trust and confidence. QCI, in collaboration with NCIIPC, has developed the Conformity Assessment Framework (CAF). This framework is structured into three tiers:

- Basic Technical Criteria (Level 1) herein after referred to as BTC (Level 1)
- Supplementary Technical Criteria (Level 2) herein after referred to as STC (Level 2)
- Additional Technical Criteria (Level 3) herein after referred to as ATC (Level 3)

These tiers collectively establish a robust Cyber Security Management System (CSMS).

1.2. CSMS is a risk-based security strategy that identifies the key cyber risks to an organization's most valuable assets and prioritizes spending to mitigate those risks to an acceptable level. A security approach shaped by risk-based decisions enables an organization to develop more practical and realistic security goals, allocating resources more effectively. Risk-based security helps organizations prevent cyber-attacks and data breaches. Furthermore, it ensures compliance not as an end in itself but as a natural consequence of a strong and optimized security posture. CSEs identify controls for implementation based on the results of risk analysis.

1.3. The underlying difference between CSMS certification and inspection lies in the fact that, while CSMS focuses on processes (verification of implementation), inspection centers on testing and assessing infrastructure (validation and effectiveness). Inspection activities ensure that the 'safeguards' prescribed in the Inspection Criteria are effectively implemented for each control. Additionally, it is ensured that configurations of software and hardware adhere to industry-recommended benchmarks.

1.4. System vulnerabilities and unused services increase the attack surface of a system, creating potential entry points for attackers. An examination of the IT/ICS system design/architecture, a review of the inventory (including hardware, software, firmware, OS, etc.), and determination of their conformity with a specific security posture facilitate addressing the aforementioned challenge. A hardened system at various levels enables the implementation of a 'Defense-in-Depth' approach. The assurance of system hardening is generally achieved through technical examination against public benchmarks, performed through inspection (testing and assessment). This necessitates the establishment of an inspection scheme for IBs.

1.5. As cyber-attacks pose a significant threat to CII, it is crucial to establish both necessary and sufficient requirements. Therefore, a 'Defense-in-Depth' assurance approach is recommended to enhance the security and resilience of the information system.

1.6. The requirements mandated in this Scheme are not mutually exclusive with the CSMS scheme and complement the requirements specified in BTC (Level 1), STC (Level 2) and ATC (Level 3). CSMS and inspection activities are strongly coupled/connected, and each inspection control supports a control defined in CSMS. Therefore, it becomes a complementary activity to make the whole assurance process more robust and

trustworthy.

1.7. This scheme is dedicated to designing and developing inspection criteria for Cyber Security based on ISO/IEC 17020:2012. It will be operationalized through accredited third-party Inspection Bodies (IBs).

2. Objective

The scheme is designed to strengthen the security and robustness of CII. It provides a structured approach for CSEs to fortify their systems against possible cyber-attacks by establishing vulnerability scanning, system hardening, and subsequently validating the robustness through penetration testing conducted by an approved third-party Inspection Body (IB).

The objective of this document is to:

2.1. Describe life cycle activities associated with the conformance activity of 'inspection.' The requirements mandated in this document will facilitate managing and controlling the inspection, which shall be carried out by practitioners employed by IBs. These practitioners are capable of using their professional judgment objectively, as per the scope of work.

2.2. Provide a uniform approach to the inspection of various CSEs.

2.3. Provide a roadmap to the CSEs to harden their IT and ICS infrastructure.

3. Scope

3.1 The overall scope of this document covers inspection life cycle processes, which include defining inspection criteria, application, inspection planning, the conduct of inspection, and its frequency for a CSE and surveillance. It also encompasses approval systems and rules for the use of the Scheme Mark for the IB.

3.2 This document's technical scope encompasses security controls related to inspection requirements in both IT and ICS environments.

4. Structure of the document

This document is divided into seven sections, as under:

Section 1: Introduction
Section 2: Governing Structure
Section 3: Inspection Criteria
Section 4: Inspection Process
Section 5: Requirements for Inspection Bodies
Section 6: Provisional Approval System
Section 7: Rules for use of Scheme Mark

5. Approach and concept

5.1 The purpose of this document is to assist organizations in planning and conducting technical information security tests and examinations, analyzing findings, and developing mitigation strategies.

5.2 These tools can serve various purposes, including identifying vulnerabilities in a system or network, verifying compliance with information security policies, and meeting other requirements for security testing and examination. This overview focuses on key elements of technical security testing and examination, emphasizing specific technical techniques rather than providing detailed technical information.

5.3 In designing this document, the following concepts are used:

5.3.1 ISO defines *Inspection* as the examination of a product design, product, or installation to determine its conformity with specific requirements, or based on professional judgment, under general conditions. Similarly, *Examine* is defined as the generation of a verdict through analysis using evaluator expertise. In the context of IT/ICS, this concept is manifested as information security testing and assessment.

5.3.2 An information security assessment is the process of determining how effectively an entity (e.g., host, system, network, procedure, personnel referred to as an assessment object) meets specific security objectives. Three types of assessment methods can be used to accomplish this, namely testing, examination, and interviews.

5.3.3 *Testing* is a process of accessing one or two assessment objects under specified conditions to compare actual and expected behaviours.

5.3.4 *Examination* is the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence.

5.3.5 *Interviewing* is the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or identify the location of evidence (e.g., during architecture review). Assessment results are used to support the determination of security control effectiveness over time.
Source NIST 800-115.

Note: ISO and NIST have used the concept of ‘inspection’ v/s ‘testing and assessment’ indicating the same intent in the context of IT/ICS.

6. Glossary

The definitions in this document are provided for reference purposes and should be interpreted in accordance with the definitions outlined in ISO/IEC 27000 and its family of standards.

6.1 **Accreditation** - Third-party attestation related to a conformity assessment body, providing a formal demonstration of its competence to perform specific conformity assessment tasks.

6.2 **Accreditation Body** - An authoritative body responsible for performing accreditation. The authority of an accreditation body may be derived from the government, public authorities, contracts, market acceptance, or scheme owners.

6.3 **Approval** - The permission granted for a product or process to be marketed or used for stated purposes or under specified conditions. This authorization is contingent upon the fulfilment of specified requirements or the completion of specified procedures.

6.4 **Asset -** Anything that holds value for an individual, organization, or government.

6.5 **Asset Owner** – An individual or company responsible for one or more assets.

6.6 **Assessment** - A process of evaluating an individual's fulfilment of the requirements of the scheme.

6.7 **Benchmark** – A reference point against which comparisons can be made.

6.8 **Complaint** - An expression of dissatisfaction, other than an appeal, made by any person or organization to a conformity assessment body or accreditation body. This pertains to the activities of that body, and a response is expected.

6.9 **Conformity Assessment** - The demonstration that specified requirements are fulfilled. It includes activities defined elsewhere in this document, such as, but not limited to, testing, inspection, validation, verification, certification, and accreditation.

6.10 **Conformity Assessment Body** – A body that performs conformity assessment activities, **excluding** accreditation. The CAF includes the following conformity assessment bodies:

6.10.1 Certification Body (CB)

6.10.2 Inspection Body (IB)

6.10.3 Certification Body for Persons (PrCB)

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

6.12 **Conformity Assessment System** - A set of rules and procedures designed for the management of similar or related conformity assessment schemes. Such a system can operate at international, regional, national, sub-national, or industry sector levels.

6.13 **Conformity Assessment Scheme** - A set of rules and procedures that describe the objects of conformity assessment, identify specified requirements and provide the methodology for performing conformity assessment. A scheme can be managed within a conformity assessment system and operated at the international, regional, national, sub-national, or industry sector level. It may cover all or part of the conformity assessment functions.

6.14 **Critical Information Infrastructure (CII)-** A computer resource, the incapacitation or destruction of which would have a debilitating impact on national security, the economy, public health, or safety.

6.15 **Critical Asset -** An asset that significantly influences the operation of the power supply system. The unavailability of such assets impacts the reliability and operability of the power supply system.

6.16 **Critical Sector** – A Critical Sector that has been officially designated as crucial to the nation by the appropriate authority.

6.17 **Critical Sector Entity (CSE)** – Entities within critical sectors, whose assets, systems, and networks are so vital that their incapacitation or destruction would have a debilitating impact on national security, the economy, public health, public safety, or any combination thereof.

6.18 **Cyber Asset** - the programmable electronic devices, including the hardware, software and data in those devices that are connected over a network, such as LAN, WAN and HAN

6.19 **Cyber Security** - Safeguarding information, equipment, devices, computer resources, communication devices, and the information stored therein from unauthorized access, use, disclosure, disruption, modification, or destruction, as defined by the Information Technology Act, 2000 (as amended by the Information Technology (Amendment) Act, 2008).

The interdependent network of information technology infrastructures includes the

Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.
This complex environment emerges from the interaction of people, software, and services on the Internet through technology devices and connected networks, yet it does not exist in any physical form.

6.20 **Examine -** To generate a verdict by analysis using evaluator expertise.

6.21 **Hardening -** A process intended to eliminate potential attack vectors by patching vulnerabilities and disabling nonessential services.
Source- NIST SP 800-152

6.22 **Inspection -** An examining a product's design, the product itself, or an installation to determine its conformity with specific requirements. This determination is made either through adherence to explicit criteria or, when professional judgment is applied, in accordance with general conditions.

6.23 **Information Security** - The preservation of the confidentiality, integrity, and availability of information. Additionally, other properties such as authenticity, accountability, non-repudiation, and reliability may also be considered (ISO 27000:2018). It encompasses the protection of information and information systems against unauthorized access, use, disclosure, disruption, modification, or destruction to ensure confidentiality, integrity, and availability (NIST SP 800-53 Rev 5)

6.24 **Information Technology** - The technology, encompassing computer systems, networks, and software, that is utilized for the processing, storage, acquisition, and distribution of information.

6.25 **Mark Holder-** Entities that are authorized to use the Scheme Mark, and these include Conformity Assessment Bodies (CAB), such as Inspection Bodies.

6.26 **Mark Owner**- The individual or organization responsible for developing, issuing, and managing the Scheme Mark.

6.27 **Network-Assisted Auditing -** Network-assisted auditing techniques may include, for example, teleconferencing, web meetings, interactive web-based communications, and remote electronic access to the CSMS documentation or CSMS processes. The focus of these techniques shall be to enhance audit effectiveness and efficiency while supporting the integrity of the audit process.

6.28 **Object of Conformity Assessment** - The entity to which specified requirements apply. This entity can take various forms, such as a product, process, service, system, installation, project, data, design, material, claim, person, body, or organization, either individually or in combination. Within this framework, the term "body" is utilized to denote both conformity assessment bodies and accreditation bodies. The term "organization" is employed in its general sense and may encompass bodies according to the context.

6.29 **Policy -** An overall intention expressed by the management.

6.30 **Provisional Approval -** Approval given to a CB meeting the criteria specified in this document, which has been awarded for the time being to develop its capabilities for formal compliance and accreditation.

6.31 **Provisional Approval Criteria -** criteria defined to award provisional approval, which gives a minimum level of confidence that CB will be able to provide contractually agreed certification services within the defined scope.

6.32 **Review** - Verification of the suitability, adequacy and effectiveness of selection and determination activities, and the results of these activities, about the fulfilment of specified requirements by an object of conformity assessment.

6.33 **Robustness** - The persistence of a system's characteristic behaviour under perturbations or conditions of uncertainty.

6.34 **Scheme Mark -** A protected mark owned by QCI (on behalf of NCIIPC), indicating that the mark holder conforms with specified requirements of the Scheme. The “Scheme

Mark" is also commonly known as a "Logo", however for the sake of aligning it with the international requirements the same will henceforth be referred to as the "Mark".

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

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

6.37 **Transmission System -** Transmission grid for the transport of electrical energy using a high voltage or ultra-high voltage grid or a gas transmission network for the transport of natural gas using a high-pressure pipeline network.

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

6.39 **Vulnerability** - Weakness of an asset or control that could potentially be exploited by one or more threats.

7. Abbreviations

Abbreviation	Acronym
AB	Accreditation Body
AT	Assessment Team
ATC	Additional Technical Criteria
BTC	Basic Technical Criteria
CAB	Conformity Assessment Body
CAF	Conformity Assessment Framework
CB	Certification Body
CC	Certification Committee
CERT-In	Indian Computer Emergency Response Team
CIA	Confidentiality, Integrity and Availability
CII	Critical Information Infrastructure
CIP	Critical Infrastructure Protection
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CO	Consultancy Organisation
CSE	Critical Sector Entity
CSMS	Cyber Security Management System for IT/ ICS
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain Name System
DRR	Disaster Risk Reduction
IAF	International Accreditation Forum
IB	Inspection Body
ICS	Industrial Control System
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IG	Implementation Group

IS	Indian Standards
ISO	International Organisation for Standardisation
ISMS	Information Security Management System
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MFA	Multi-factor Authentication
MSC	Multi-stakeholder committee
NABCB	National Accreditation Board for Certification Bodies
NCIIPC	National Critical Information Infrastructure Protection Centre
NIST	National Institute of Standards and Technology
NSAB	National Security Advisory Board
NSCS	National Security Council Secretariat
NTRO	National Technical Research Organisation
OEM	Original Equipment Manufacturer
OT	Operational Technology
PII	Personal Identifiable Information
QCI	Quality Council of India
SC	Steering Committee
SCADA	Supervisory Control and Data Acquisition
SCAP	Security Content Automation Protocol
SIEM	Security Information and Event Management
SO	Scheme Owner
SoC	Statement of Compliance
SOP	Standard Operating Procedure
SPOC	Single Point of Contact
SSH	Secure Shell
STC	Supplementary or Sector Technical Criteria
TB	Training Body
TC	Technical Committee
VPC	Virtual Private Cloud

SECTION 2

GOVERNING STRUCTURE

1. Objective

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

2. Scheme Owner and Scheme Manager

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

2.1 Roles and Responsibilities of the Scheme Owner

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

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

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

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

a. Ensure that information about the Scheme is made publicly available, and 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, particularly the responsibilities for governance of the Scheme.
c. The ownership of the 'Scheme Mark' (logo) must be duly registered with the appropriate authority. Inspection bodies and inspected entities are required to obtain formal approval for the use of the Mark.
d. Handle complaints at all levels (stakeholders, public) regarding the quality of products as well as the Scheme operation.
e. Participate in all meetings of Committees - Steering, Technical, and Certification Committees, as needed for the development and management of the Scheme.

2.2 Roles and Responsibilities of the Scheme Manager

2.2.1 Responsible for all activities related to the 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 the conformity assessment activity and the criteria selected for the approval of the IBs.

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 IBs to ensure that the IBs 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 IBs 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 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 IBs are processed expeditiously. Investigation and decision on complaints shall not result in any discriminatory actions.

Note 1: A description of the complaints handling process will be publicly available with or without request.

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

2.2.10 Oversee the implementation of the changes (e.g., transition period) made by the IBs' 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 (the National Accreditation Body and Scheme Manager) on behalf of NCIIPC (the Scheme Owner).

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

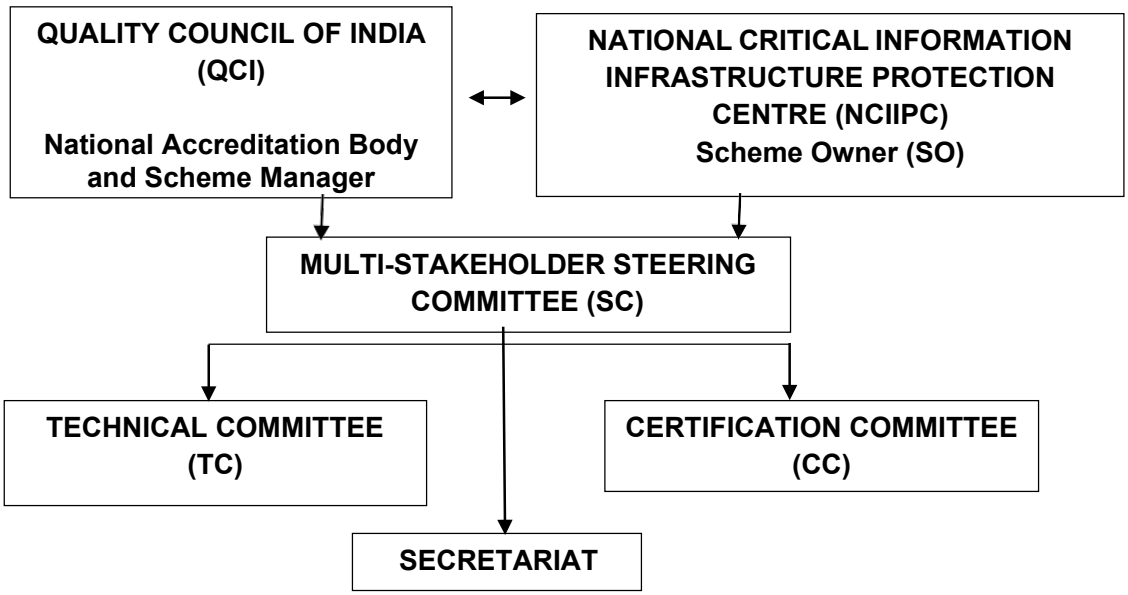

Figure 2.1: Governing Structure

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.

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

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

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

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

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

3.3.9 Minutes of the meeting are to be issued by the Secretary of the committee with the 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 prepare the document for the respective Committee's review, input, and approval. Once completed, the document will be submitted to the Committee Chair for final approval.

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 an individual capacity.

4.1.2 Nominees from the concerned ministries, regulatory bodies, and allied bodies specific to the scope of the Scheme– Representatives from the Ministries responsible for critical sectors, namely banking, financial services, insurance, telecom, government, power and energy, transport, strategic enterprises, and healthcare, representatives from the regulatory bodies responsible for the critical sectors, such as the Central Electricity Authority (CEA), Reserve Bank of India (RBI) etc.

4.1.3 Government Agencies – Representatives 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 the 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 committee meetings will be issued by the committee's Secretary with the 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 – Chairperson – a person of eminence, can be in an 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 the Scheme Owner. Further representatives of similar organisations may be called by rotation as per requirement and mutual agreement by Chairperson TC, Scheme Owner.

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 IBs.

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 an 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 the 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 inspection process and requirements for IBs for IBs to apply for accreditation.

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

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

6.2.5 Deliberations on any other issue relating to the inspection of IBs.

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 the Scheme Owner. It shall establish the MSC in consultation with the Scheme Owner and shall be responsible for the overall management of the Scheme. QCI shall provide the Secretariat to the Scheme.

7.3 National Accreditation Board for Certification Bodies (NABCB), a constituent Board of the QCI, shall be responsible for accrediting IBs desirous of participation in the Scheme. NABCB shall, through a legally enforceable agreement with the accredited IB, ensure that the IB shall offer NABCB and its representatives, including assessors, experts, observers, and regulators appointed in the assessment teams, such reasonable access and cooperation, as necessary, enable NABCB assessment team to monitor conformity with the Agreement and the relevant standard(s). The accredited IB shall also grant access to NABCB assessors, experts, and observers to its premises for conducting assessment activities. The level of access granted to NCIIPC personnel, or any personnel nominated by them will be equivalent to that provided to NABCB.

8. Complaints

8.1 A complaint is an expression of dissatisfaction, other than an appeal, by any person or organization to an IB 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 IBs and ABs are required to have a complaints system in place as per the 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 an IB to the AB for reconsideration of a decision made by that body.

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

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

handle it.

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

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

9.6 The statement of appeal received by the NCIIPC will be forwarded to QCI. QCI will then process the appeal and may choose to present it at each MSC 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 review process shall also encompass an examination of past performance data pertaining to approved IBs, as well as an assessment of the status of complaints, appeals, RTIs, and any other relevant information.

SECTION 3

INSPECTION CRITERIA

1. Objective

1.1 To enable all the Critical Sector Entities to implement a common set of controls for hardening their IT/ICS infrastructure.

1.2 To identify a set of Inspection Criteria in order to assess:

- the benchmarks are implemented
- vulnerabilities are patched
- non-essential services are turned off
- validation by VA/PT

through an independent technically competent body known as an Inspection Body to provide confidence to CSEs that their IT/ICS infrastructure is secured and fortified against cyber-attacks.

2. Scope

This document provides a set of controls to be implemented by the CSEs for their IT and ICS infrastructure to fortify against cyber-attacks, thereby achieving the organization's cybersecurity goals.

Additionally, the document includes references for assessment and test report formats, to bring uniformity by various IBs in reporting the status of VA/PT.

3. Intended Stakeholders

3.1 Inspection Bodies (IBs)

3.2 Any CSEs in the critical sector seeking inspection reports from IBs, and CSMS Implementers. CBs may also refer to this document before planning for the CSMS audit.

3.3 Inspectors of Inspection Body.

3.4 Accreditation Body.

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

3.6 Authorized Training bodies and Consulting Organizations as well as National bodies that are mandated for tasks related to cybersecurity of Critical Sectors.

3.7 OEMs, Suppliers, Vendors, Software Developers and System Integrators of IT, SCADA, ICS systems and other components, which are being used in the Critical Sector.

3.8 Academic Institutions, Cybersecurity Professionals, and other interested stakeholders - Personnel and Entities.

4. References for Implementation Guidance

The following documents, in whole or in part, are normatively referenced in inspection criteria for IT and ICS.

4.1 Normative References

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

4.1.2 Center for Internet Security (CIS) - Controls and Benchmarks (v7.0) for ICS infrastructure. Informative References

4.2 Informative References

4.2.1 NIST 800-115 - Technical Guide to Information Security Testing and Assessment

4.2.2 NIST 800-171 - Guidelines for Protecting Sensitive Information

4.2.3 NIST 800-167 - Guide to Application Whitelisting

4.2.4 NIST 800-41 - Guidelines on Firewalls and Firewall Policy

4.2.5 NIST 800-53 - Security and Privacy Controls for Information Systems and Organizations

4.2.6 NIST 800-128 - Guide for Security-Focused Configuration Management of Information Systems

4.2.7 NIST 800-123 - Guide to General Server Security

4.2.8 NIST 800-124 - Guidelines for Managing the Security of Mobile Devices in the Enterprise

5. Document Structure and Principles

5.1 Overview of Inspection Criteria for IT Systems.

The Inspection Criteria for IT are adopted from CIS v8.0 which are described below:

(List of IT controls with description)
(Ref. document: CIS v8.0)

These 18 controls share insights into attacks and attackers, identify root causes, and translate that into classes of defensive action and are described below:

S No.	Control	Description
1.	Inventory and Control of Enterprise Assets	Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.
2.	Inventory and Control of Software Assets	Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.
3.	Data Protection	Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.
4.	Secure Configuration of Enterprise Assets and Software	Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile, network devices, non-computing/IoT devices, and servers) and software (operating systems and applications).
5.	Account Management	Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.
6.	Access Control Management	Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.
7.	Continuous Vulnerability Management	Develop a plan to continuously assess and track vulnerabilities across all enterprise assets within the infrastructure. This aims to promptly remediate and minimize the window of opportunity for potential attackers. Monitor public and private industry sources for new threats and vulnerability information.

S No.	Control	Description
8.	Audit Log Management	Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.
9.	Email and Web Browser Protections	Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers To manipulate human behavior through direct engagement.
10.	Malware Defenses	Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.
11.	Data Recovery	Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.
12.	Network Infrastructure Management	Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.
13.	Network Monitoring and Defense	Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.
14.	Security Awareness and Skills Training	Establish and maintain a security awareness program to influence behaviour among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.
15.	Service Provider Management	Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.
16.	Application Software Security	Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.
17.	Incident Response Management	Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.
18.	Penetration Testing	Test the effectiveness and resiliency of enterprise assets by identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

Note: These 18 controls are to be validated by the Inspection Team by using vulnerability scanners, penetration testing tools, scenario creations and other techniques focusing on infrastructure without auditing the processes. Some of these activities may be required to be jointly undertaken by the CISO and inspection team.

The details of controls and safeguards are provided in Annex A of this section. consisting of 18 CIS (v8.0) controls for IT infrastructure with normative descriptions. This annexure may be used to map the controls prescribed in Basic Technical Criteria (Level 1).

Annex C of this section consists of the mapping of CIS controls with IS/ISO/IEC 27001:2022 which is informative.

5.2 Overview of controls for Industrial Control System (ICS)

S No.	Control	Description
1.	Inventory and Control of Hardware Assets	This control addresses the challenges in ICS which are mixtures of old and new devices from multiple vendors, network segmentation, dual-homing, isolation, lack of up-to-date diagrams, unique industry, and application-specific protocols, some of which are not IP-based, and the difficulty in conducting physical inventories in dispersed or hostile environments. It focuses on Understanding and solving the asset inventory and device visibility problem which are critical in managing a business' security program.
2.	Inventory and Control of Software Assets	This CIS Control offers steps needed to identify, track, and account for software in a network. It offers active management of software that can be a challenge in ICS. Much of the software is provided by vendors and is tied to hardware levels. This software often has commercially available components that are also tied to the hardware. Large parts of ICS networks are comprised of devices too sensitive to scan or unable to support endpoint software.
3.	Continuous Vulnerability Management	It assists in understanding and managing vulnerabilities that are just as challenging to an ICS environment as it is to traditional IT systems. Additionally, differences in ICS lifecycle and vendor support can overlap with software obsolescence, causing periods where no updates exist. These scenarios are identified as part of the vulnerability scanning control and mitigations or upgrade plans which are put into place.
4.	Controlled Use of Administrative Privileges	This addresses the need for limiting and managing administrator access. One of the two primary ways for attackers to spread inside a system is by tricking a user with elevated credentials into opening an email attachment, downloading, and running an infected file, or visiting a malicious website from an asset connected to the ICS.
5.	Secure Configurations for Hardware and Software on Devices, Laptops, Workstations, and Servers	This control provides guidance for securing hardware and software. Many modern ICS logic and visualization platforms operate on common operating systems and many benchmarks and hardening guides exist. It is also important to consider OEM and vendor recommendations in terms of the standard security configuration for all manufacturer-provided operating systems and software.
6.	Maintenance, Monitoring, and Analysis of Audit Logs	This control offers guidance for the maintenance and monitoring of audit logs. Logging of security events in ICS environments can be a challenge due to the nature of many of the embedded or legacy devices present. Many devices do not support native logging of security events.

7.	Email and Web Browser Protection	This control focuses on the security of web browsers and email clients, which are very vulnerable attack vectors. Most ICS environments do not require Internet web access and email clients are not needed because they are often isolated from business networks. Email is utilized in ICS environments but typically only in an outgoing manner.
8.	Malware Defense	This control addresses the steps needed to ensure a strong defense against malware intrusions. Malicious code is a very real threat to ICS. It has been crafted to target the devices or processes unique to these industries. Additionally, many devices do not support endpoint software, thus making on-device malware monitoring difficult which is addressed by this control.
9.	Limitations and Control of Network Ports, Protocols, and Services	This control focuses on the need for controlling network access points, ports, and services. When accounting for ports, protocols, and services, it is often helpful to start from vendor documentation since many ICSs comprise proprietary systems. Many vendors or OEMs have baseline documentation that can provide a starting point or details specific to their solutions.
10.	Data Recovery Capabilities	This control references the need for performing system backups for data recovery capability. It requires different approaches within individual ICS environments. Different components support various backup methods. While some support full system backups, the majority offer only configuration exports. Still others may offer no capability to export configurations.
11.	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	This control addresses the need to manage the configuration of all network devices using a change control process. The network infrastructure of an ICS network typically carries additional requirements when compared to traditional IT systems. Usually, these networks focus on availability and are architected with real-time performance and redundancy requirements. Attack vectors, however, remain the same. Insecure services, poor firewall configurations, and default credentials remain issues.

12.	Boundary Defense	This control focuses on the importance of managing the flow of information between networks of different trust levels. Alignment with the Purdue Reference Model 2 should be the primary goal when measuring the security architecture's effectiveness in an ICS network. When following this model, any ICS networks that require Internet connectivity should utilize a proxy. This proxy should not be dual-homed, nor perform as a bastion host, and it should reside within a less trusted.
13.	Data Protection	This control's focus is on data protection and the relevance greatly varies based on the ICS environment. These environments often do not contain much if any sensitive data in the traditional sense (PII, Credit Cards, etc.) In many ICS networks, control data consists of physical measurements such as flow, temperature, pressure, or valve readings and specific commands issued by logic control devices that control an overall process.
14.	Controlled Access Based on the Need to Know	The need to control access to systems based on the need to know is critically important. When following proper network layering (see the Purdue Reference Model), some degree of physical and logical segmentation will be in place. Devices that directly measure or control physical processes are typically segmented from general-purpose workstations. These references should align with the data protection control. This may remove applicability parts of this Control depending on the ICS environment.
15.	Wireless Access Control	This control references the security of wireless access points. Networks with wireless access points can be accessed from outside the physical building where security controls may be present. Likewise, rogue access points can be used to gain unrestricted access to internal ICS networks. The presence and type of wireless networks vary depending on the ICS vertical industry, application type, owner & operator requirements, and desires, and even per laws and regulations when specialized wireless equipment is employed. Some OT teams use wireless where devices need to be mobile or when spread out.
16.	Account Monitoring and Control	This control emphasizes the importance of controlling user access to systems in a typical network environment and ensuring effective account management. Additionally, remote and on-premises contractors and OEM technicians often request or require access either locally or remotely. These factors can make managing user accounts difficult for many OT teams, especially over a period of time given competing priorities for systems to be operating in a productive state, versus being idle for service and maintenance.

17.	Implement a Security Awareness and Training Program	This control focuses on educating and training the typical enterprise workforce in a range of security practices that span basic to advanced skills to security awareness and vigilance. The experience and pedigree of third-party resources should be carefully evaluated, including evaluation and validation of purported knowledge, skills, and abilities (KSAs) before allowing said third parties access to critical components and systems.
18.	Application Software Security	This control focuses on application security in the OT environment, where countless off-the-shelf, web-based, and proprietary applications can be running on a network. This can be a big task for system administrators. It is not uncommon for ICS environments to contain some custom-engineered, in-house built web-based, or other application software that is specialized for the given system. Such applications and services may not always follow a disciplined engineering development, test, and maintenance process.
19.	Incident Response and Management	This control addresses the processes and steps required to prepare for an incident. Well-defined and implemented incident response plans can allow an enterprise to identify, contain, reduce impacts, and more quickly recover from a cyber incident. This is especially important for organizations where ICS downtime can lead to safety, health, or profitability impacts affecting the company, employees, customers, supply chain partners, community, and other constituents depending on the safe, reliable operation of an organization.
20.	Penetration Tests and Red Team Exercises	This control is focused on designing and conducting controlled penetration testing in an operational technology environment, including connected devices and systems that may not be normally viewed as a constituent component, service, or system for an ICS. Processes controlled by ICS environments are easily disrupted by penetration testing, red team exercises, or other similar activities. Performing these activities on production systems, even during scheduled outages, can lead to downtime, destruction, and injury, or introduce lingering artifacts that reduce the safety, efficiency, or performance of the tested system. Hence, it is highly recommended to only perform penetration testing and red-team exercises on non-production systems such as lab equipment, during scheduled downtime, or factory acceptance testing when proper oversights and precautions are before a system is installed.

5.2.1 The operational environment of the ICS system poses unique requirements not addressed by the CIS controls.

5.2.2 ICS are facing security challenges demanding additional controls. Many of the core security concerns are shared both by IT and ICS. ICS systems typically operate software and hardware that directly control physical equipment and processes, compounding this issue is the fact that many of the systems not only often have high availability requirements, but also are often the underpinning of critical infrastructure.ICS system relies heavily on a combination of open and proprietary technologies provided by OEM products, systems, and services. Asset owners generally have an agreement with OEMs/ SP/ SI for after-sales support across the operation phase. These include configuration setting, system hardening, providing patches, port setting and penetration testing as they demand extensive domain knowledge, and technical insights and may impact ICS operations. However, such agreements often impose restrictions on ICS asset owners for what adjustments they can make to ICS without voiding the warranty. Therefore, these agreements must be considered when determining how to implement safeguards to harden ICS systems and solutions.
CIS controls for ICS are described above in 5.2:

Annex B (of this section): 20 CIS (v7.0) controls for ICS infrastructure with description (Normative) Implementation Guidance:
NIST has published a set of implementation guidance which is referred to in Cl 4.2 as an Informative reference above. CSEs may use these as per applicability.

6. Rationale for selecting CIS Cyber Security controls for Inspection Criteria:

CIS Controls are more prescriptive and pragmatic and have a wider industry acceptance. These controls include the following elements:

- Overview (brief description)
- Reasons for the controls being critical.
- Procedure and tools
- Safeguard descriptions

The controls are used on an ‘as is’ basis. The rationale and implementation guidelines prescribed in reasons for the controls being critical and procedures and tools are not reproduced in this document. Readers may refer to the CIS document for exploration in this regard.

6.1 The CIS controls are a prioritized set of actions that collectively form a defense-in-depth set of best practices that help in mitigating the most common attacks on the ICS systems and networks.

6.2 These controls share insight into attacks and attackers, identify root causes, and translate that into classes of defensive actions.

6.3 These controls are bundled in control **Implementation Groups (IGs)** as detailed below:

6.3.1 **Implementation Group 1 (IG1)** indicates CIS sub-controls for small, commercial off-the-shelf or home office software environments where the sensitivity of the data is low will typically fall under IG1. An organization with limited cybersecurity expertise and available resources can implement these sub-controls.

6.3.2 **Implementation Group 2 (IG2)** indicates CIS sub-controls focused on helping security teams manage sensitive client or company information fall under IG2. IG2 steps should also be followed by organizations in IG3. An organization with moderate cybersecurity expertise and resources are necessary to implement these sub-controls.

6.3.3 **Implementation Group 3 (IG3)** indicates CIS sub-controls that reduce the impact of zero-day attacks and targeted attacks from sophisticated adversaries typically fall into IG3. For a mature organization with significant cybersecurity experience, resources are essential to allocate to these sub-controls.

IG1 is essential to cyber hygiene, the foundational set of cyber defense safeguards that every CSE should apply to guard against the most common attacks. Each IG then builds up upon the previous one e.g. IG2 includes IG1 and IG3 includes all CIS safeguards in IG2. For CII, all controls i.e. IG3 are essential unless and until any particular control is not applicable and the same shall be documented in the SoA process (documenting rationale and obtaining management approval). This grouping, primarily, facilitates and guides the sequence of implementation. (IG1⟹ IG2 ⟹IG3) IG1 and IG2 organizations may be unable to implement all IG3 sub-controls.

The distribution of safeguards for each control for various IGs (ICS v8 for IT systems) are mentioned below:

Control	Safeguard	IG1	IG2	IG3
1.	5	2	4	5
2.	7	3	6	7
3.	14	6	12	14
4.	12	7	11	12
5.	6	4	6	6
6.	8	5	7	8
7.	7	4	7	7
8.	12	3	11	12
9.	9	2	6	7
10.	7	3	7	7
11.	5	4	5	5
12.	8	1	7	8
13.	11	0	6	11
14.	9	8	9	9

15.	7	1	4	7
16.	14	0	11	14
17.	9	3	8	9
18.	5	0	3	5

The distribution of safeguards for each control for various IGs (ICS v7.1 for ICS systems) is mentioned below, which are adopted from version 'v 7/v 7.1 CIS Controls: Implementation Guide for Industrial Control Systems' available at www.cisecurity.org. Some of the safeguards/ sub-controls may not be applicable depending on the deployed architecture and ICS infrastructure) (Refer to Annex B of this Section)

Control	Safeguard	IG1	IG2	IG3
1.	8	2	6	8
2.	10	3	5	10
3.	7	2	7	7
4.	9	2	8	9
5.	5	1	5	5
6.	8	1	7	8
7.	10	2	9	10
8.	8	3	8	8
9.	9	1	4	5
10.	5	4	5	5
11.	7	1	7	7
12.	12	2	8	12
13.	9	3	5	9
14.	9	1	5	9
15.	10	2	7	9
16.	13	3	12	13
17.	9	6	9	9
18.	11	0	10	11
19.	8	4	7	8
20.	8	0	6	8

For CII, it is essential to implement all the IGs which are IG1, IG2 and IG3.

7. Relationship between CSMS Technical Criteria and Inspection Criteria

7.1 The conformity assessment framework for CSEs consists of CSMS at three levels viz.,

BTC (Level 1), STC (Level 2) and ATC (Level 3) and Inspection Scheme.

The CSMS is a risk-based management framework which helps CSEs to identify, analyse and address cyber security risks to protect against cyber threats and data breaches and focuses on management system requirements supported by a list of controls mentioned in Annex A of Basic Technical Criteria (Level 1). This annexure facilitates the selection of controls depending on the applicability also known as the 'Statement of Applicability'.

The core framework is based on a six-step planning process that involves collaboration between several different departments within an organisation and other stakeholders, as applicable. It primarily covers defining cyber security policy, scope of CSMS, conduct of risk assessment and management of identified risks as well as risk-based selection of controls.

7.2 At this stage, it is required to establish cybersecurity capabilities which have the biggest impact, in reducing risks more substantially than the subsequent activities. As the organisation matures and capabilities advance, additional improvements result in less risk reduction, and decisions may require more consideration of the organisation's specific objectives.

7.3 CIS has defined a framework consisting of 18 critical security controls to provide smaller, prioritised no. of specific and actionable controls focused on technology that should be implemented first to yield immediate results rather than implementing numerous controls. These prioritised controls will help CSEs to focus on vital requirements to establish a baseline for protection and cyber defense. These controls are focused on technical implementation to harden CSE cyber security, while CSMS is a management system that needs these controls but requires a management layer to support these controls with additional controls. CIS control doesn't have any management layer. Since these controls are a part of technical implementation, they need to be assured by testing and assessment methodologies generally carried out by IBs against inspection criteria.

7.4 The controls of CSMS and inspection criteria are strongly coupled. Each control defined in inspection criteria can be mapped to CSMS control in one way or another to a great extent (sometimes a sub-set equally or a superset of it combining or splitting of controls) The conformity assessment approach is different.

7.5 This requirement of inspection criteria is justified as it is a short-term thrust providing immediate and intense impacts whereas the CSMS is justified because it is a long-term approach containing a formal management system which is sustainable and capable of addressing an ever-changing landscape of threats and vulnerabilities in a CSE.

7.6 It is recommended that organisations should start implementing controls pertaining to inspection criteria to harden their infrastructure. Further, this framework facilitates implementation in 3 steps of implementation (IG 1, IG 2 and IG 3) Once the infrastructure is hardened and validated by inspection reports (which include VA/PT reports), organisations shall start designing and implementing CSMS i.e. BTC (Level 1), STC (Level 2) and ATC (Level 3) in the respective order. The principles of inspection criteria are common for all the three levels of CSMS hence not specified level-wise. However, specific implementation guidelines have been provided for the ICS environment.

7.7 Organisations that have already been certified and/or compliant with ISO/IEC 27001:2022 (ISMS) and working on CSMS for BTC (Level 1), can implement inspection criteria concurrently. However, their assessment (CSMS and inspection) shall be carried out by the respective team of experts/AT.

7.8 The structure of inspection criteria is focused on practices termed as 'Safeguards' whereas the controls specified in BTC (Level 1) are at a higher-level requiring policy, processes, mechanisms etc. Since source frameworks are different hence there lies a variation in such presentation.

Annexure A

List of IT controls with safeguard and description (indicating Asset Type and Title)
(Ref. document: CIS v8.0)

CIS Control	CIS Safeguard	Asset Type	Title	Description
1	**Inventory and Control of Enterprise Assets**			
1	1.1	Devices	Establish and Maintain Detailed Enterprise Asset Inventory	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to including end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM-type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under the control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.
1	1.2	Devices	Address Unauthorized Assets	Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.

CIS Control	CIS Safeguard	Asset Type	Title	Description
	1.3	Devices	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.
1	1.4	Devices	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.
1	1.5	Devices	Use a Passive Asset Discovery Tool	Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.
1	**Implementation guidelines**			a. Establish a mechanism to have comprehensive & dynamic visibility over the asset. b. Ensure that the asset on-boarding process, including the procurement process is revitalized to incorporate security principles [factoring security implications, security requirements, security configurability, & implementation considerations] c. Ensure that the asset management program/mechanism extends the coverage to all assets and asset types that can potentially create security ramifications. d. Ensure a life cycle approach for managing assets and their security. e. Record cryptographic strength of assets [for devising plans of Crypto Agility]

CIS Control	CIS Safeguard	Asset Type	Title	Description
2	2.1	Applications	Establish and Maintain a Software Inventory	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.
2	2.2	Applications	Ensure Authorized Software is Currently Supported	Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfilment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate it as unauthorized. Review the software list to verify software support at least monthly, or more frequently.
2	2.3	Applications	Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.
2	2.4	Applications	Utilize Automated Software Inventory Tools	Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.
2	2.5	Applications	Allowlist Authorized Software	Use technical controls, such as application allow listing, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.
2	2.6	Applications	Allow list Authorized Libraries	Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process.

CIS Control	CIS Safeguard	Asset Type	Title	Description
				Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.
2	2.7	Applications	Allowlist Authorized Scripts	Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.
2	**Implementation guidelines**			a. Ensure Software Bill of Materials [SBOM] is maintained for software by stating requirements [if procuring] or mandating [if developing internally]. b. Ensure visibility over the Cryptographic Modules and Algorithms implemented in software. c. Ensure a mechanism for discovering and recording open-source components/ libraries/ capabilities/ modules.
3	**Data Protection**			
3	3.1	Data	Establish and Maintain a Data Management Process	Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
3	3.2	Data	Establish and Maintain a Data Inventory	Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.

CIS Control	CIS Safeguard	Asset Type	Title	Description
3	3.3	Data	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.
3	3.4	Data	Enforce Data Retention	Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.
3	3.5	Data	Securely Dispose of Data	Securely dispose of data as outlined in the enterprise's data management process. Ensure the disposal process and method are commensurate with the data sensitivity.
3	3.6	Devices	Encrypt Data on End-User Devices	Encrypt data on end-user devices containing sensitive data. Example implementations can include Windows BitLocker®, Apple FileVault®, and Linux® dm-crypt.
3	3.7	Data	Establish and Maintain a Data Classification Scheme	Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.

CIS Control	CIS Safeguard	Asset Type	Title	Description
3	3.8	Data	Document Data Flows	Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise's data management process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
3	3.9	Data	Encrypt Data on Removable Media	Encrypt data on removable media.
3	3.10	Data	Encrypt Sensitive Data in Transit	Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).
3	3.11	Data	Encrypt Sensitive Data at Rest	Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.
3	3.12	Network	Segment Data Processing and Storage Based on Sensitivity	Segment data processing and storage based on the sensitivity of the data. Do not process sensitive data on enterprise assets intended for lower sensitivity data.
3	3.13	Data	Deploy a Data Loss Prevention Solution	Implement an automated tool, such as a host-based Data Loss Prevention (DLP) tool to identify all sensitive data stored, processed, or transmitted

CIS Control	CIS Safeguard	Asset Type	Title	Description
				through enterprise assets, including those located onsite or at a remote service provider, and update the enterprise's sensitive data inventory.
3	3.14	Data	Log Sensitive Data Access	Log sensitive data access, including modification and disposal.
3	**Implementation Guidelines**			a. Ensure a mechanism for discovering, identifying, and preventing data loss. b. Deploy a mechanism for maintaining and managing data security posture. c. Ensure that activity associated with data is monitoring and baselined for identifying abnormal behaviour.
4	**Secure Configuration of Enterprise Assets and Software**			
4	4.1	Applications	Establish and Maintain a Secure Configuration Process	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
4	4.2	Network	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
4	4.3			Configure automatic session locking on enterprise assets after a defined period of inactivity. For general-purpose operating systems,

CIS Control	CIS Safeguard	Asset Type	Title	Description
			Configure Automatic Session Locking on Enterprise Assets	the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.
4	4.4	Devices	Implement and Manage a Firewall on Servers	Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, an operating system firewall, or a third-party firewall agent.
4	4.5	Devices	Implement and Manage a Firewall on End-User Devices	Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.
4	4.6	Network	Securely Manage Enterprise Assets and Software	Securely manage enterprise assets and software. Example implementations include managing configuration through version- controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.
4	4.7	Users	Manage Default Accounts on Enterprise Assets and Software	Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include disabling default accounts or making them unusable.

CIS Control	CIS Safeguard	Asset Type	Title	Description
4	4.8	Devices	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file-sharing service, web application module, or service function.
4	4.9	Devices	Configure Trusted DNS Servers on Enterprise Assets	Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.
4	4.10	Devices	Enforce Automatic Device Lockout on Portable End- User Devices	Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts.
4	4.11	Devices	Enforce Remote Wipe Capability on Portable End- User Devices	Remotely wipe enterprise data from enterprise-owned portable end-user devices when deemed appropriate such as lost or stolen devices, or when an individual no longer supports the enterprise.
4	4.12	Devices	Separate Enterprise Workspaces on Mobile End-User Devices	Ensure separate enterprise workspaces are used on mobile end-user devices, where supported. Example implementations include using an Apple® Configuration Profile or Android™ Work Profile to separate enterprise applications and data from personal applications and data.
4	**Implementation Guidelines**			Carry breach and attack simulations and adversarial emulation exercises against the hardening standards.

CIS Control	CIS Safeguard	Asset Type	Title	Description
5	**Account Management**			
5	5.1	Users	Establish and Maintain an Inventory of Accounts	Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.
5	5.2	Users	Use Unique Passwords	Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.
5	5.3	Users	Disable Dormant Accounts	Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.
5	5.4	Users	Restrict Administrator Privileges to Dedicated Administrator Accounts	Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.
5	5.5	Users	Establish and Maintain an Inventory of Service Accounts	Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain the department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are

CIS Control	CIS Safeguard	Asset Type	Title	Description
				authorized, on a recurring schedule at a minimum quarterly, or more frequently.
5	5.6	Users	Centralize Account Management	Centralize account management through a directory or identity service.
5	**Implementation Guidelines**			a. Ensure a mechanism for managing privileged users and their access. b. Monitor behaviour for establishing normal behaviour and trigger responses for abnormal user and entity behaviour
6	**Access Control Management**			
6	6.1	Users	Establish an Access Granting Process	Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.
6	6.2	Users	Establish an Access Revoking Process	Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.
6	6.3	Users	Require MFA for Externally- Exposed Applications	Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.

CIS Control	CIS Safeguard	Asset Type	Title	Description
6	6.4	Users	Require MFA for Remote Network Access	Require MFA for remote network access.
6	6.5	Users	Require MFA for Administrative Access	Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.
6	6.6	Users	Establish and Maintain an Inventory of Authentication and Authorization Systems	Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.
6	6.7	Users	Centralize Access Control	Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.
6	6.8	Data	Define and Maintain Role- Based Access Control	Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges areauthorized, on a recurring schedule at a minimum annually, or more frequently.
6	**Implementation Guidelines**			a. Ensure a mechanism for identifying and baselining behaviours of users and entities to identify abnormal behaviour and trigger necessary enforcement actions b. Ensure all necessary and contemporary security precautions in managing active directory Wireless Access Control: c. Ensure a mechanism for profiling and baselining the behaviour of

CIS Control	CIS Safeguard	Asset Type	Title	Description
				wireless devices connecting to the network to identify and trigger enforcement actions on abnormal activities
7	**Continuous Vulnerability Management**			
7	7.1	Applications	Establish and Maintain a Vulnerability Management Process	Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
7	7.2	Applications	Establish and Maintain a Remediation Process	Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
7	7.3	Applications	Perform Automated Operating System Patch Management	Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
7	7.4	Applications	Perform Automated Application Patch Management	Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
7	7.5	Applications	Perform Automated Vulnerability Scans of Internal Enterprise Assets	Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.

CIS Control	CIS Safeguard	Asset Type	Title	Description
7	7.6	Applications	Perform Automated Vulnerability Scans of Externally Exposed Enterprise Assets	Perform automated vulnerability scans of externally exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.
7	7.7	Applications	Remediate Detected Vulnerabilities	Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
7	**Implementation Guidelines**			a. Deploy ways and mechanisms for prioritizing vulnerabilities based on the risk posed by the organizations. b. Deploy Risk Quantification Method/Mechanism contextual to threat exposure.
8	**Audit Log Management**			
8	8.1	Network	Establish and Maintain an Audit Log Management Process	Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
8	8.2	Network	Collect Audit Logs	Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.
8	8.3	Network	Ensure Adequate Audit Log Storage	Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.

CIS Control	CIS Safeguard	Asset Type	Title	Description
8	8.4	Network	Standardize Time Synchronization	Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.
8	8.5	Network	Collect Detailed Audit Logs	Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.
8	8.6	Network	Collect DNS Query Audit Logs	Collect DNS query audit logs on enterprise assets, where appropriate and supported.
8	8.7	Network	Collect URL Request Audit Logs	Collect URL request audit logs on enterprise assets, where appropriate and supported.
8	8.8	Devices	Collect Command-Line Audit Logs	Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.
8	8.9	Network	Centralize Audit Logs	Centralize, to the extent possible, audit log collection and retention across enterprise assets.
8	8.10	Network	Retain Audit Logs	Retain audit logs across enterprise assets for a minimum of 90 days.

CIS Control	CIS Safeguard	Asset Type	Title	Description
8	8.11	Network	Conduct Audit Log Reviews	Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.
8	8.12	Data	Collect Service Provider Logs	Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events.
8	**Implementation Guidelines**			Ensure that any issue/vulnerability/weakness creating larger ramification is detected timely and triggers proportionate and swift response to limit damage and recovery effectively
9	**Email and Web Browser Protections**			
9	9.1	Applications	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.
9	9.2	Network	Use DNS Filtering Services	Use DNS filtering services on all enterprise assets to block access to known malicious domains.
9	9.3	Network	Maintain and Enforce Network-Based URL Filters	Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation- based filtering, or through the use of block lists. Enforce filters for all enterprise assets.

CIS Control	CIS Safeguard	Asset Type	Title	Description
9	9.4	Applications	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	Restrict, either through uninstalling or disabling, any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.
9	9.5	Network	Implement DMARC	To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.
9	9.6	Network	Block Unnecessary File Types	Block unnecessary file types attempting to enter the enterprise's email gateway.
9	9.7	Network	Deploy and Maintain Email Server Anti-Malware Protections	Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.
9	**Implementation Guidelines**			a. Ensure that secure content management is enforced even if the IT asset is connected to a public network. b. Ensure a mechanism for Dynamic categorization of URL and content, real-time risk analysis of uncategorized sites and pages, and the categorization of search results
10	**Malware Defenses**			
10	10.1	Devices	Deploy and Maintain Anti- Malware Software	Deploy and maintain anti-malware software on all enterprise assets.

CIS Control	CIS Safeguard	Asset Type	Title	Description
10	10.2	Devices	Configure Automatic Anti- Malware Signature Updates	Configure automatic updates for anti-malware signature files on all enterprise assets.
10	10.3	Devices	Disable Autorun and Autoplay for Removable Media	Disable autorun and autoplay auto-execute functionality for removable media.
10	10.4	Devices	Configure Automatic Anti- Malware Scanning of Removable Media	Configure anti-malware software to automatically scan removable media.
10	10.5	Devices	Enable Anti-Exploitation Features	Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.
10	10.6	Devices	Centrally Manage Anti- Malware Software	Centrally manage anti-malware software.
10	10.7	Devices	Use Behavior-Based Anti- Malware Software	Use behavior-based anti-malware software.
10	**Implementation Guidelines**			Deploy a mechanism for understanding behaviour of file/fileless code/ malware and protecting from abnormal behaviour.

CIS Control	CIS Safeguard	Asset Type	Title	Description
11	**Data Recovery**			
11	11.1	Data	Establish and Maintain a Data Recovery Process	Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
11	11.2	Data	Perform Automated Backups	Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.
11	11.3	Data	Establish and Maintain an Isolated Instance of Recovery Data	Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services.
11	11.4	Data	Test Data Recovery	Test backup recovery quarterly, or more frequently, for a sampling of in-scope enterprise assets.
11	**Implementation Guidelines**			a. Ensure backup solutions are ransomware-proof b. Ensure that the recovery solution supports managed recovery c. Ensure that recovery capabilities support recovering secrets
12	**Network Infrastructure Management**			

CIS Control	CIS Safeguard	Asset Type	Title	Description
12	12.1	Network	Ensure Network Infrastructure is Up-to-Date	Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.
12	12.2	Network	Establish and Maintain a Secure Network Architecture	Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.
12	12.3	Network	Securely Manage Network Infrastructure	Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.
12	12.4	Network	Establish and Maintain Architecture Diagram(s)	Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
12	12.5	Network	Centralize Network Authentication, Authorization, and Auditing (AAA)	Centralize network AAA.
12	12.6	Network	Use of Secure Network Management and Communication Protocols	Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).

CIS Control	CIS Safeguard	Asset Type	Title	Description
12	12.7	Devices	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure	Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end- user devices.
12	12.8	Devices	Establish and Maintain Dedicated Computing Resources for All Administrative Work	Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.
12	**Implementation Guidelines**			a. Ensure content and context awareness and behaviour-based actions in network security, and application level firewall and introduction detection and prevention b. Ensure content and context awareness and behaviour-based actions in network security, and application level firewall and introduction detection and prevention
13	**Network monitoring and Defenses**			
13	13.1	Network	Centralize Security Event Alerting	Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.

CIS Control	CIS Safeguard	Asset Type	Title	Description
13	13.2	Devices	Deploy a Host-Based Intrusion Detection Solution	Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.
13	13.3	Network	Deploy a Network Intrusion Detection Solution	Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.
13	13.4	Network	Perform Traffic Filtering Between Network Segments	Perform traffic filtering between network segments, where appropriate.
13	13.5	Devices	Manage Access Control for Remote Assets	Manage access control for assets remotely connecting to enterprise resources. Determine the amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.
13	13.6	Network	Collect Network Traffic Flow Logs	Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.
13	13.7	Devices	Deploy a Host-Based Intrusion Prevention Solution	Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include the use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.

CIS Control	CIS Safeguard	Asset Type	Title	Description
13	13.8	Network	Deploy a Network Intrusion Prevention Solution	Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.
13	13.9	Devices	Deploy Port-Level Access Control	Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.
13	13.10	Network	Perform Application Layer Filtering	Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.
13	13.11	Network	Tune Security Event Alerting Thresholds	Tune security event alerting thresholds monthly, or more frequently.
13	**Implementation Guidelines**			Boundary Defence: a. Ensure a mechanism for baselining and profiling benign/ normal traffic identifying anomalies and triggering necessary enforcement actions. b. Establishing continuous visibility over the inbound and outbound traffic reflects the dynamic understanding of an organization about inbound and outbound linkages.
14	**Security Awareness and Skills Training**			

CIS Control	CIS Safeguard	Asset Type	Title	Description
14	14.1	N/A	Establish and Maintain a Security Awareness Program	Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.
14	14.2	N/A	Train Workforce Members to Recognize Social Engineering Attacks	Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.
14	14.3	N/A	Train Workforce Members on Authentication Best Practices	Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.
14	14.4	N/A	Train Workforce on Data Handling Best Practices	Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.
14	14.5	N/A	Train Workforce Members on Causes of Unintentional Data Exposure	Train workforce members to be aware of causes for unintentional data exposure. Example topics include the mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.

CIS Control	CIS Safeguard	Asset Type	Title	Description
14	14.6	N/A	Train Workforce Members on Recognizing and Reporting Security Incidents	Train workforce members to be able to recognize a potential incident and be able to report such an incident.
14	14.7	N/A	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	Train the workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.
14	14.8	N/A	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure.
14	14.9	N/A	Conduct Role-Specific Security Awareness and Skills Training	Conduct role-specific security awareness and skills training. Example implementations include secure system administration courses for IT professionals, (OWASP® Top 10 vulnerability awareness and prevention training for web application developers, and advanced social engineering awareness training for high-profile roles.

CIS Control	CIS Safeguard	Asset Type	Title	Description
14	***Implementation Guidelines***			a. Deploy a mechanism for testing/ simulating users and their responses to phishing attacks. b. Ensure that training and awareness are delivered contextual to the user role, contextual to the situation, and based on behaviour demonstrated by the user.
15	**Service Provider Management**			
15	15.1	N/A	Establish and Maintain an Inventory of Service Providers	Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard.
15	15.2	N/A	Establish and Maintain a Service Provider Management Policy	Establish and maintain a service provider management policy. Ensure the policy addresses the classification, inventory, assessment, monitoring, and decommissioning of service providers. Review and update the policy annually, or when significant enterprise changes occur that could impact this Safeguard.
15	15.3	N/A	Classify Service Providers	Classify service providers. Classification consideration may include one or more characteristics, such as data sensitivity, data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. Update and review classifications annually, or when significant enterprise changes occur that could impact this Safeguard.
15	15.4	N/A	Ensure Service Provider Contracts	Ensure service provider contracts include security requirements. Example requirements may include minimum security program requirements, security incident and/or data breach notification and response, data encryption requirements, and data disposal commitments. These security requirements

CIS Control	CIS Safeguard	Asset Type	Title	Description
			Include Security Requirements	must be consistent with the enterprise's service provider management policy. Review service provider contracts annually to ensure contracts are not missing security requirements.
15	15.5	N/A	Assess Service Providers	Assess service providers consistent with the enterprise's service provider management policy. Assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. Reassess service providers annually, at a minimum, or with new and renewed contracts.
15	15.6	Data	Monitor Service Providers	Monitor service providers consistent with the enterprise's service provider management policy. Monitoring may include periodic reassessment of service provider compliance, monitoring service provider release notes, and dark web monitoring.
15	15.7	Data	Securely Decommission Service Providers	Securely decommission service providers. Example considerations include user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.
15	**Implementation Guidelines**			N/A
16	**Application Software Security**			
16	16.1	Applications	Establish and Maintain a Secure Application	Establish and maintain a secure application development process. In the process, address such items as secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and

CIS Control	CIS Safeguard	Asset Type	Title	Description
			Development Process	update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
16	16.2	Applications	Establish and Maintain a Process to Accept and AddressSoftware Vulnerabilities	Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process includes such items as a vulnerability handling policy that identifies the reporting process, the responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. Third-party application developers need to consider this an externally facing policy that helps to set expectations for outside stakeholders.
16	16.3	Applications	Perform Root Cause Analysis on Security Vulnerabilities	Perform root cause analysis on security vulnerabilities. When reviewing vulnerabilities, root cause analysis is the task of evaluating underlying issues that create vulnerabilities in code and allows development teams to move beyond just fixing individual vulnerabilities as they arise.
16	16.4	Applications	Establish and Manage an Inventory of Third-Party Software Components	Establish and manage an updated inventory of third-party components used in development, often referred to as a “bill of materials,” as well as components slated for future use. This inventory is to include any risks that each third-party component could pose. Evaluate the list at least monthly to identify any changes or updates to these components and validate that the component is still supported.

CIS Control	CIS Safeguard	Asset Type	Title	Description
16	16.5	Applications	Use Up-to-Date and Trusted Third-Party Software Components	Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.
16	16.6	Applications	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities	Establish and maintain a severity rating system and process for application vulnerabilities that facilitate prioritizing the order in which discovered vulnerabilities are fixed. This process includes setting a minimum level of security acceptability for releasing code or applications. Severity ratings bring a systematic way of triaging vulnerabilities that improves risk management and helps ensure the most severe bugs are fixed first. Review and update the system and process annually.
16	16.7	Applications	Use Standard Hardening Configuration Templates for Application Infrastructure	Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.
16	16.8	Applications	Separate Production and Non-Production Systems	Maintain separate environments for production and non-production systems.
16	16.9	Applications	Train Developers in Application Security Concepts and Secure Coding	Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. Training can include general security principles and application security standard practices. Conduct training at least annually and design in a way to promote security within the development team, and build a culture of security among the developers.

CIS Control	CIS Safeguard	Asset Type	Title	Description
16	16.10	Applications	Apply Secure Design Principles in Application Architectures	Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.
16	16.11	Applications	Leverage Vetted Modules or Services for Application Security Components	Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.
16	16.12	Applications	Implement Code-Level Security Checks	Apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed.
16	16.13	Applications	Conduct Application Penetration Testing	Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.

CIS Control	CIS Safeguard	Asset Type	Title	Description
16	16.14	Applications	Conduct Threat Modeling	Conduct threat modeling. Threat modelling is the process of identifying and addressing application security design flaws within a design before code is created. It is conducted through specially trained individuals who evaluate the application design and gauge security risks for each entry point and access level. The goal is to map out the application, architecture, and infrastructure in a structured way to understand its weaknesses.
16	**Implementation Guidelines**			a. Set up an application security governance mechanism to ensure that vulnerabilities and weaknesses are timely identified and issues are resolved promptly. b. Ensure a mechanism for understanding, mapping, and analysing software composition. c. Set up a process for backward tracing of application modules, libraries, and functionalities, including decisions made for security and privacy.
17	**Incident Response Management**			
17	17.1	N/A	Designate Personnel to Manage Incident Handling	Designate one key person, and at least one backup, who will manage the enterprise's incident-handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.
17	17.2	N/A	Establish and Maintain Contact Information for Reporting Security Incidents	Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC)

CIS Control	CIS Safeguard	Asset Type	Title	Description
				partners, or other stakeholders. Verify contacts annually to ensure that information is up to date.
17	17.2	N/A	Establish and Maintain Contact Information for Reporting Security Incidents	Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up to date.
17	17.3	N/A	Establish and Maintain an Enterprise Process for Reporting Incidents	Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.
17	17.4	N/A	Establish and Maintain an Incident Response Process	Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.
17	17.5	N/A	Assign Key Roles and Responsibilities	Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard.
17	17.6	N/A	Define Mechanisms for Communicating	Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters. Keep in mind that certain mechanisms, such

CIS Control	CIS Safeguard	Asset Type	Title	Description
			During Incident Response	as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.
17	17.7	N/A	Conduct Routine Incident Response Exercises	Plan and conduct routine incident response exercises and scenarios for key personnel involved in the incident response process to prepare for responding to real-world incidents. Exercises need to test communication channels, decision-making, and workflows. Conduct testing on an annual basis, at a minimum.
17	17.8	N/A	Conduct Post-Incident Reviews	Conduct post-incident reviews. Post-incident reviews help prevent incident recurrence by identifying lessons learned and follow-up. action.
17	17.9	N/A	Establish and Maintain Security Incident Thresholds	Establish and maintain security incident thresholds, including, at a minimum, differentiating between an incident and an event. Examples can include abnormal activity, security vulnerability, security weakness, data breaches, privacy incidents, etc. Review annually, or when significant enterprise changes occur that could impact this Safeguard.
17	**Implementation Guidelines**			Ensure that playbooks for all critical possible incident scenarios are documented and response mechanism is configured to bring systematization and predictability to the response.
18	**Penetration Testing**			
18	18.1	N/A	Establish and Maintain a Penetration Testing Program	Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded

CIS Control	CIS Safeguard	Asset Type	Title	Description
				attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.
18	18.2	Network	Perform Periodic External Penetration Tests	Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be a clear box or an opaque box.
18	18.3	Network	Remediate Penetration Test Findings	Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.
18	18.4	Network	Validate Security Measures	Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing.
18	18.5	N/A	Perform Periodic Internal Penetration Tests	Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box.
18	**Implementation Guidelines**			Incorporate breach simulation, adversarial emulation, threat hunting, and attack surface management to test the strength of security preparedness.

Annexure B

List of CIS controls for ICS infrastructure with description

(v7.0/ v7.1)

Note: This is adopted from version 'v 7/v 7.1 CIS Controls: Implementation Guide for Industrial Control Systems' available at www.cisecurity.org. Some of the safeguards/ sub-controls may not be applicable depending on the deployed architecture and ICS infrastructure)

CIS Control 1 – Inventory and Control of Hardware Assets	
Introduction	The first CIS Control is considered to be the most important because it's necessary to first identify the systems and devices that need to be secured. CIS Control 1 is about taking inventory. Understanding and solving the asset inventory and device visibility problem is critical in managing a business' security program. This is especially challenging in ICS where network segmentation, dual-homing, and isolation are common themes. Mixtures of old and new devices from multiple vendors, lack of up-to-date diagrams, unique industry, and application-specific protocols, some of which are not IP-based, and the difficulty in conducting physical inventories in dispersed or hostile environments compound these challenges
Applicability	The conventional approach of using ping responses, TCP SYN or ACK scans can also be problematic in ICS due to device sensitivity since even seemingly benign scanning employed in IT environments can disrupt communications, or in some cases even impact device operations. Methods that are more passive in locating connected assets are preferred, as they are less likely to impact system availability or interact with vendor systems in a manner that could cause warranty issues. Where practical, non-intrusive methods should be leveraged including MAC-ARP tables, DNS, active directory, or a variety of ICS-specific tools employed to control and collect data in these systems all for the purpose of locating the variety of connected assets. Network-level authentication via 802.1x does not work on many of the devices found in ICS, which do not support supplicant software. Network-level authentication can cause reliability issues if not strictly maintained. Instead, consider a non-802.1x network access approach that is more ICS device-friendly and can at a minimum alert of new devices detected on the network. • Sub-controls related to network-level authentication may not be applicable to ICS environments. • Sub-Controls related to client-based certificates may not be applicable to ICS environments. • Certificate-based authentications in PKI environments can be complex and expensive.

Considerations	Considerations For this CIS Control consider the following additional steps: • Consider the lifecycle and acquisition costs, for example, NIST 800-82r2: Component Lifetime. Typical IT components have a lifetime on the order of 3 to 5 years, with brevity due to the quick evolution of technology. For ICS, where technology has been developed for very specific use and implementation, the lifetime of the deployed technology is often 10 to 15 years and sometimes longer. • Ensure that all equipment acquisitions and system modifications follow an approval process and the technical drawings (if applicable, automated inventory systems) are updated at the time of the change
Implementation guidelines	a. Establish a mechanism to have comprehensive & dynamic visibility over the asset. b. Ensure that the asset on-boarding process, including the procurement process is revitalized to incorporate security principles *[factoring security implications, security requirements, security configurability, & implementation considerations]* c. Ensure that the asset management program/mechanism extends the coverage to all assets and asset types that can potentially create security ramifications. d. Ensure a life cycle approach for managing asset and their security.
CIS Control 2 – Inventory and Control of Software Assets	
Introduction	This CIS Control offers steps needed to identify, track, and account for software in a network. Actively managing software can be a challenge in ICS. Much of the software is provided by vendors and is tied to hardware levels. This software often has commercially available components that are also tied to the hardware. Furthermore, applying patches to the operating systems and software applications can introduce new variables that lead to incompatibilities and even disruption or potential for loss or damage to data, product, equipment, and the safety of personnel. Using automated software inventory tools can also pose a challenge in ICS. Many collection methods rely on active scanning or endpoint software. Large parts of ICS networks are comprised of devices too sensitive to scan or unable to support endpoint software.
Applicability	Sub-controls related to air-gapped systems and network isolation may not be applicable. Due to the network communication requirements of many ICS software, true isolation may not be possible. Additionally, depending on OEM vendor offering and support, virtualization may not be supported. Instead, utilize transparent firewalls or sub-netwide segmentation to mitigate high-risk applications. Exercise caution when considering automated software inventory tools as these may cause stability issues on some systems. Many ICS devices may not support or be too sensitive to these tool's collection methods. For Sub-Control(s) related to whitelisting, utilize application whitelisting technology only where feasible. Depending on system criticality, unauthorized software can be alerted or blocked from executing on systems. For embedded devices that utilize firmware, leverage firmware signing (or something similar) if available.

Considerations	For this CIS Control consider the following additional steps: a. Ensure ICS manufacturers and vendors provide a list of recommended and supported software and versions that are required for each system. b. Forecast operating systems and application lifecycle cost in alignment with typical COTS (commercial off-the-shelf software) End of Life and End of Support (EoL/EoS) Notifications. c. Ensure cybersecurity requirements are a consideration within procurement/sourcing processes. Specifically, d. ensure vendors leverage a secure development lifecycle.
Implementation Guidelines	a. Ensure Software Bill of Materials [SBOM] is maintained for software by stating requirements [if procuring] or mandating [if developing internally] b. Ensure visibility over the Cryptographic Modules and Algorithms implemented in software. c. Ensure a mechanism for discovering and recording open sources components/ libraries/ capabilities/ modules.
CIS Control 3 – Continuous Vulnerability Management	
Introduction	This CIS Control addresses the need for continuous vulnerability management, which can be a significant task in most organizations. Understanding and managing vulnerabilities is just as challenging to an ICS environment as it is to traditional IT systems. One advantage the ICS has in this arena is that these systems typically reside farther into a business's network layers making it harder for external threat actors to reach and exploit new vulnerabilities without first telegraphing some presence inside the system when monitoring is in place. However, the required up-time on ICS means that the service and maintenance windows where updates can be applied are limited and sometimes months (or years) apart. Additionally, differences in ICS lifecycle and vendor support can overlap with software obsolescence, causing periods where no updates exist. These scenarios should be identified as part of the vulnerability scanning control and mitigations or upgrade plans should be put into place.
Applicability	Sub-Controls(s) related to automated scanning and patching may not be applicable in the ICS environment.
Considerations	When performing active vulnerability scanning, caution should be exercised as it can adversely affect ICS network communications and in turn, product and system availability. There are several reasons for this, including network stack sensitivity, limited resources, or other situational factors. Scanning should only take place during process outages such as regular scheduled maintenance or during planned shutdowns. Furthermore, steps should be taken (for example: reboot or

	restart critical services) to ensure there are no unintended side effects. Ensure that tools do not automatically deploy software. These tools should report and identify where security updates are needed but allow the OT team to deploy updates when it is safe to do so. For this CIS Control consider the following additional steps: a. In addition to traditional channels, utilize an OEM vulnerability reporting service to identify all known vulnerabilities on the organization's ICS. b. Utilize passive monitoring tools which identify a specific device and software version and correlate that to known vulnerabilities. c. Operating system and application updates, security patches, and service packs need to be properly regression tested to ensure the availability and reliability of the system will not be adversely affected. Where possible, have the OEM regression test completed prior to OT team testing. d. Create a test bed that mimics a production environment for specific patch regression testing prior to implementing it in production OT environments.
Implementation Guidelines	a. Deploy ways and mechanisms for prioritizing vulnerabilities based on the risk posed by the organizations. b. Deploy Risk Quantification Method/Mechanism contextual to threat exposure.
CIS Control 4 – Controlled Use of Administrative Privileges	
Introduction	This CIS Control addresses the need for limiting and managing administrator access. One of the two primary ways for attackers to spread inside a system is by tricking a user with elevated credentials into opening an email attachment, downloading and running an infected file, or visiting a malicious website from an asset connected to the ICS. As per Control 7, these externally-enabled attack vectors should not be present on ICS networks. The method of guessing or cracking a password is still a valid concern, especially due to older devices that lack adequately engineered authentication and authorization mechanisms that recognize and protect against brute force attacks. Because of these differences, a handful of Sub-Controls should not be implemented in an ICS environment.
Applicability	Sub-Controls related to the use of multi-factor authentication may be possible for crossing boundaries but may not be possible with the internal ICS environment. Sub-Controls related to the use of automated tools that alert when new users are added may not be applicable. Sub-Controls related to the use of dedicated machines or the use of isolation for administrator machines may not be applicable. When inventorying all administrative accounts, automated tools are not
Considerations	For this CIS Control consider the following additional steps: a. Minimize the use of elevated privileges and only use administrative accounts where they are required.

Implementation Guidelines	a. Ensure a mechanism for managing privilege users and their access. b. Monitor behaviour for establishing normal behaviour and trigger responses for abnormal user and entity behaviour.
CIS Control 5 – Secure Configurations for Hardware and Software on Devices, Laptops, Workstations, and Servers	
Introduction	This CIS Control provides guidance for securing hardware and software. Many modern ICS logic and visualization platforms operate on common operating systems and many benchmarks and hardening guides exist. It is also important to consider OEM and vendor recommendations in terms of the standard security configuration for all manufacturer-provided operating systems and software. Additionally, many ICS devices do not fit into the categories mentioned in CIS Control 3 or 11 but should still have some level of secure configurations. At a minimum, and where possible, these devices should have unused services and ports disabled, default accounts changed, and protocols updated, and be examined for other ways to reduce the devices' attack surface. When this is not possible, monitoring should be employed to detect and alert unusual activities that may be suspect.
Applicability	All the Sub-Controls are applicable.
Considerations	It is recommended that when configuration management tools are used, they be set to alert-only without automated configuration re-deployment unless it is known to be safe to do so
Implementation Guidelines	Carry breach and attack simulations and adversarial emulation exercises against the hardening standards
CIS Control 6 – Maintenance, Monitoring, and Analysis of Audit Logs	
Introduction	This CIS Control offers guidance for the maintenance and monitoring of audit logs. Logging of security events in ICS environments can be a challenge due to the nature of many of the embedded or legacy devices present. Many devices do not support native logging of security events. Those that do often do not inherently support sending those events to an external device such as a central logging server so special action may need to be taken to gain access to such information.
Applicability	All Sub-Controls are applicable. However, many systems or devices may not support the level of logging recommended by this Control.

Considerations	If looking to leverage an IT-based SIEM, make sure it supports the ICS environment because many logging analytic and alerting solutions do not support or correctly interpret or correlate ICS specific events.
Implementation Guidelines	Ensure that any issue/vulnerability/weakness creating larger ramification is detected timely and triggers proportionate and swift response to limit damage and recovery effectively.
CIS Control 7 – Email and Web Browser Protection	
Introduction	This CIS Control focuses on the security of web browsers and email clients, which are very vulnerable attack vectors. Most ICS environments do not require Internet web access and email clients are not needed because they are often isolated from business networks. Email is utilized in ICS environments but typically only in an outgoing manner. It is common to have systems that monitor critical processes and send out alerts or reports via email. These emails are typically accessed from business or corporate assets that are on separate networks and have no access to the ICS environment. While Internet web access is not required, often services are provided via internal web servers. Therefore, unlike email clients, web browsers may still be required, but the risk posed by these browsers is greatly reduced as an attacker would have to first compromise the internal web server.
Applicability	Most of the Sub-Controls are not applicable to the ICS environment for the reasons stated above. However, Sub-Controls related to using authorized browsers for business purposes are applicable. The key is restricting web access.
Considerations	In cases where certain Sub-Controls are not applicable, the following additional requirements should be enforced: • Ensure that all systems are segmented such that there is no Internet web access. • Ensure that no email clients are installed or present on any systems. Where a device or system has the capability to send email-based alerts or reports, ensure that it is limited to outbound only.
Implementation Guidelines	a. Ensure that secure content management is enforced even if the IT asset is connected to a public network. b. Ensure a mechanism for Dynamic categorization of URL and content, real-time risk analysis of uncategorized sites and pages, and the categorization of search results.
CIS Control 8 – Malware Defense	

Introduction	This CIS Control addresses the steps needed to ensure a strong defense against malware intrusions. Malicious code is a very real threat to ICS. It has been crafted to target the devices or processes unique to these industries. While proper network segmentation and defense-in-depth strategies help to mitigate this risk by making it difficult for threat actors to deliver malware to their intended locations, malware defense still needs tools and processes in place to detect incidents. Unfortunately, the sensitivity and critical nature of these environments make it difficult to regularly update Antivirus definitions for fear the update process might impact the reliability of critical systems. Additionally, many devices do not support endpoint software, thus making on-device malware monitoring difficult.
Applicability	All Sub-Controls are applicable.
Considerations	For this CIS Control consider the following additional steps: a. Anti-malware tools need to be properly regression-tested to ensure that availability and reliability of the system will not be adversely affected. This testing should take place whenever a change is made to the anti-malware software such as a configuration change, software hotfix, or repository update. b. Ensure anti-malware tools are configured such that a false positive detection will not negatively impact the availability or reliability of any critical processes. Some OT teams may not want to incur the risk of updating c. antivirus definitions while critical processes are running. Consider, at a minimum, performing software updates
Implementation Guidelines	Deploy a mechanism for understanding behaviour of file/fileless code/malware and protecting from abnormal behaviour. When scanning removable media, it is recommended that the content be scanned before it can be accessed, but not upon insertion. By scanning on insertion, larger portable storage devices can take a significant time to finish scanning and impede productivity. However, by scanning prior to access, content can be scanned on demand and have less of an impact on productivity. Anti-exploitation features can be very challenging to implement. Much of the industry's proprietary software has not been designed to leverage operating systems' memory protection features. Other devices simply cannot support these technologies. Some third-party packages can enable anti- exploitation functionality to supported devices. However, they can often create resource overhead that may impact the real-time requirements of these systems. While anti-exploitation technologies are valuable, they should only be applied where they are innately supported or do not impact the performance of ICS.
CIS Control 9 – Limitations and Control of Network Ports, Protocols, and Services	

Introduction	This CIS Control focuses on the need for controlling network access points, ports, and services. When accounting for ports, protocols and services, it is often helpful to start from vendor documentation since many ICS comprise proprietary systems. Many vendors or OEM have baseline documentation that can provide a starting point or details specific to their solutions.
Applicability	All Sub-Controls are applicable.
Considerations	When inventorying open or available network ports, the process or tools used should be non-intrusive and not impact the availability or reliability of the system. In the ICS environment, most systems are considered critical and mail servers should not be present in ICS networks.
CIS Control 10 – Data Recovery Capabilities	
Introduction	This CIS Control references the need for performing system backups for data recovery capability. It requires different approaches within individual ICS environments. Different components support various backup methods. While some support full system backups, the majority offer only configuration exports. Still others may offer no capability to export configurations.
Applicability	All the Sub-Controls are applicable.
Considerations	For this CIS Control consider the following additional steps: • Ensure that system backups and recovery procedures are documented. In terms of back-ups, most ICS systems do not support complete automatic backups, and the scheduling of these backups might cause ICS performance. Where this is the case, ensure backups are taken as appropriate. Additionally, some device configurations remain static and rarely change. In these situations, backups may only need to be performed.

Implementation Guidelines	a. Ensure backup solution are ransomware proof b. Ensure that recovery solution supports managed recovery c. Ensure that recovery capabilities support recovering secrets when configurations or data changes are made. Nonetheless, it remains important to evaluate even configurations that are expected to remain unchanged because any alteration could be an indicator of accidental/unintentional alteration, tampering or malicious intent. In cases where devices are not capable of complete backups, all software, settings, and configurations should be captured such that all information necessary to perform a restoration is known and available
CIS Control 11 – Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	
Introduction	This CIS Control addresses the need to manage the configuration of all network devices using a change control process. The network infrastructure of an ICS network typically carries additional requirements when compared to traditional IT systems. Usually these networks focus on availability and are architected with real-time performance and redundancy requirements. Attack vectors, however, remain the same. Unsecure services, poor firewall configurations, and default credentials remain issues.
Applicability	Due to the availability requirements associated with the ICS environments, Sub Controls relating to network traffic may not be applicable.
Considerations	For this CIS Control consider the following additional steps: a. Ensure firewalls are configured to deny by default. b. If a location is unmanned or if critical process data flows through a perimeter device, ensure redundancy exists or device failure won't prevent this data from being received by its intended destination. If the management environment is sufficiently isolated, then multifactor authentication may not be required to manage network devices. Adding multifactor requirements can limit the use of vendor supplied network monitoring solutions.
Implementation Guidelines	Ensure content and context awareness and behaviour based actions in network security, and application level firewall and introduction detection and prevention.

CIS Control 12 – Boundary Defense	
Introduction	This CIS Control focuses on the importance of managing the flow of information between networks of different trust levels. Alignment with the Purdue Reference Model 2 should be the primary goal when measuring the security architecture's effectiveness in an ICS network. When following this model, any ICS networks that require Internet connectivity should utilize a proxy. This proxy should not be dualhomed, nor perform as a bastion host, and it should reside within a less trusted, but still internal network (Level 4 or 5 from Purdue Model). This proxy device should be held to non-ICS security controls which may include the Sub-Controls not applicable to ICS networks. Note that a NAT or PAT firewall system is not a proxy and would not be considered an acceptable alternative.
Applicability	As stated above, ICS systems should not be directly connected to the internet. As such, any Sub-Controls referencing or inferring internet or web access are not applicable.
Considerations	For this CIS Control consider the following additional step: a. Ensure ICS and OT networks are not directly connected to the internet.

Implementation Guidelines	a. Ensure a mechanism for baselining and profiling benign/ normal traffic and identifying anomaly and triggering necessary enforcement actions b. Establish continuous visibility over the inbound and outbound traffic reflects the dynamic understanding of an organization about inbound and outbound linkages c. Maintain and enforce a minimum-security standard for all devices remotely logging into the organization's network. d. Ensure systems with multiple network interfaces are not bridging (dualhomed) the OT network with any less trusted network. e. Maintain logging of all activities and traffic that pass through this boundary, limiting services and clients to only those required to cross the security perimeter. f. Recognize that not all traffic ingress or egress may necessarily pass through one device. For this reason, it is crucial to identify all known and potential means for crossing a secure perimeter, including rogue modems, wireless devices, cellular technologies, short-range wireless connections, etc. Consider collecting network analytical data (netflow, jflow, IPFix or similar). The idea here is to collect behavioural and analytical information rather than full packet captures. Limit access to trusted and necessary IP address ranges. Denying communication with known malicious or unused internet IP addresses is not necessary, as there should be no internet-web browsing capability from within the ICS. The list of internet addresses that need to be accessed should be very short, thus a whitelist style approach would be easier to implement and maintain. It is very common in ICS environments to utilize vendor or contractor remote access. Many times, these connections come from devices or systems owned by these third parties. When this is the case, it can be difficult to scan or utilize technical controls to enforce minimum security standards. Consider using non-technical controls such as signed agreements or reports generated by the third parties to ensure minimum security standards are maintained on the devices used to remotely connect. No ICS device or network should be visible from the Internet.
CIS Control 13 – Data Protection	

Introduction	This CIS Control's focus is on data protection and the relevance greatly varies based on ICS environment. These environments often do not contain much if any sensitive data in the traditional sense (PII, Credit Cards, etc.) In many ICS networks, control data consists of physical measurements such as flow, temperature, pressure, or valve readings and specific commands issued by logic control devices that control an overall process. This information is sometimes not deemed to be especially sensitive, or proprietary on its own and in some cases it is absent of any particular protections in the way it is collected, transferred, stored, and analysed. However, some organizations consider this same information sensitive since it can indeed provide insights into an ICS design, connected products, proprietary process, production data, process variables, system schedules, configuration changes, and a bevy of other data that can provide significant intelligence to potential malefactors and wrong-doers. Some ICS environments there may be some information that is highly guarded and the ability to keep it confidential is key to the business success. This is often seen in the manufacturing space where recipes or formulas are used to make foods or chemicals. It is a growing concern for critical infrastructure ICS because it is recognized that such data leakage can aid an attacker in developing a strategy. What constitutes sensitive data is up to each OT team to assess. If it is concluded that no sensitive data is present, then this Control can be largely ignored. However, such a conclusion is expected to be a very rare exception.
Applicability	For ICS environments that do contain sensitive data, all the Sub-Controls are applicable.
Considerations	Sub-Controls related to automated and scheduled scanning might adversely affect the reliability of the system. Only scanning for sensitive data when it is safe to do so. Also, consider that encryption may not be feasible on all devices. For example, some embedded devices or network components may not be able to decrypt/encrypt data on removable media. Consider establishing a means to passively capture data from ICS using a variety of tools such as sniffers, protocol anomaly detection tools, and to periodically evaluate traffic streams for data leakage that could lead to misuse or abuse by a would-be attacker.

Implementation Guidelines	a. Ensure a mechanism for baselining and profiling benign/ normal traffic and identifying anomaly and triggering necessary enforcement actions b. Establish continuous visibility over the inbound and outbound traffic reflects the dynamic understanding of an organization about inbound and outbound linkages c. Ensure that activity of associated with data are monitoring and baselined for identifying abnormal behavior.
CIS Control 14 – Controlled Access Based on the Need to Know	
Introduction	The need to control access to systems based on the need to know is critically important. When following proper network layering (see the Purdue Reference Model), some degree of physical and logical segmentation will be in place. Devices that directly measure or control physical processes are typically segmented from general purpose workstations. However, segmentation within layers needs to also be considered. There are different approaches to network segmentation. For example, private VLANs are utilized heavily in IT and retail spaces. This approach may be applicable for ICS systems. However, consideration needs to be given to ACLs to control access and other routing requirements when provisions for remote configuration and monitoring are requirements in highly segmented systems. Segmenting by subnets is typically an acceptable approach. VLANs or dedicated switches can be used depending on availability and cost requirements. There are many references to sensitive data through this Control. These references should align with the data protection control. This may remove applicability parts of this Control depending on ICS environment.
Applicability	Sub-Controls relating to private VLANs may not be applicable. Sub-Controls relating to sensitive information or data may not be applicable.

Considerations	In general, consider physical and logical network segmentation as a means to help ensure that authorized individuals and/or systems are restricted in how they communicate with other systems necessary to fulfill their specific responsibilities. However, segmentation via VLANS is not to be considered a security control because the complexity of managing VLAN routes, inter-VLAN routing, and susceptibility for network appliances including L3 switches and routers to be misconfigured or compromised will all affect the capability for VLAN to successfully restrict traffic. Physical network segmentation has greater capability to safeguard communications and operate as a mechanism of access control and isolate communications.
Implementation Guidelines	a. Ensure a mechanism for identifying and baselining behaviours of user and entities to identify abnormal behaviour and triggering necessary enforcement actions. b. Ensure all necessary and contemporary security precautions in managing active directory
CIS Control 15 – Wireless Access Control	
Introduction	This CIS Control references the security of wireless access points. Networks with wireless access points can be accessed from outside the physical building where security controls may be present. Likewise, rogue access points can be used to gain unrestricted access to internal ICS networks. The presence and type of wireless networks vary depending on ICS vertical industry, application type, owner & operator requirements and desires, and even per laws and regulations when specialized wireless equipment is employed. Some OT teams use wireless where devices need to be mobile or when spread out. Another common scenario is wide area field mesh networks. Some teams relegate wireless to nonmission critical operations such as monitoring and diagnostics, or device and systems configuration. Some teams make broader use of wireless for even critical control operations, to connect to stranded assets, to improve device accessibility, to reduce costs, and to address limitations in available personnel, amongst other reasons.
Applicability	Sub-Controls related peer-to peer and untrusted device VLANs may not be applicable for this control.

Considerations	For this CIS Control consider the following additional steps: a. Strongly consider the ICS application and where wireless may be employed in mission critical aspects of operation that loss of communication, or a security breach may impact personal and functional safety, lead to ICS disruption, damage, or destruction of digital and physical products and services. b. Ensure wireless ICS system utilizing Public Key Infrastructure (PKI), enforce expiration dates, non-repudiation and certificate chains validation, and revocation. c. Ensure wireless (including cellular, sat, etc.) based ICS systems do not fail open when jammed. d. Ensure wireless (including cellular, sat, etc.) based ICS networks are controlled/private networks. e. Ensure software security patches and product upgrades are applied throughout the wireless infrastructure and products are kept current throughout their lifecycle. f. Recognize that wired devices do have aspects of physical security that wireless devices may not similarly enjoy. This should lead to careful consideration of whether a device must necessarily be wireless, or if wired connection is more appropriate. g. Where possible, limit wireless signal strength and range to what is necessary for the application in order to reduce the potential for remote accessibility of the connection from outside a security perimeter. References to wireless detection tools may not be applicable and should only alert on rogue devices connected to wireless access points. Profiling the device should only be done through passive means and denying device access should only be done where it won't impact the availability of the process. Use persistent, encrypted, defined point-to-point or point-to-multipoint wireless configuration. Both the base station and the remote station devices are specifically configured for secure communication. Do not permit or configure the system to allow ad hoc or guest connections.
Implementation Guidelines	Ensure a mechanism for profiling and baselining the behaviour of wireless devices connecting to the network to identify and trigger enforcement actions on abnormal activities.
CIS Control 16 – Account Monitoring and Control	

Introduction	This CIS Control emphasizes the importance of controlling user access to systems in a typical network environment and ensuring effective account management. A common vulnerability can arise if employee accounts are not closed when employees leave the organization or change roles. ICS can be equally, if not more challenging because they often contain systems from different vendors, each with their own user account directories and often inconsistent set of individuals that may interact with a system. Additionally, remote and on-premises contractors and OEM technicians often request or require access either locally or remotely. These factors can make managing user accounts difficult for many OT teams, especially over a period of time given competing priorities for systems to be operating in a productive state, versus being idle for service and maintenance. While these factors can make user account control difficult, care must be taken not to inadvertently terminate or prevent a legitimate user from having the appropriate access as this might cause process disruption or delay. Furthermore, a balance must be considered and carefully managed between administrator-only account privileges versus group level privileges. Given the 24x7x365 operation of many ICS systems, incidents can occur at any time, including during a time when there is an absence of those with administrative privileges available to respond, remediate, and recover.
Applicability	Sub-Controls related to account expiration, inactivity lockouts, and multi-factor authentication are not applicable to ICS systems.
Considerations	For this CIS Control consider the following additional steps: a. Used shared accounts and passwords only when necessary. b. Establish and follow a process for changing shared account passwords immediately upon termination of any workforce member knowing the credentials. c. Restrict shared operator account permissions to limit system access and changes. d. Where possible, eliminate ICS applications leveraging clear text authentication or basic security authentication. Where not possible, use unique credential sets and monitor for their attempted usage elsewhere. e. Consider access control chain-of-command plans for periods of time when normal personnel with required privileges may not be available. Consider monitoring the use of all accounts, automatically locking machines that are not used for process monitoring, or control after a standard period of inactivity. It is especially important f. to require the use of complex and long (14+) passwords or passphrases that are not easily guessed. Length over complexity makes current password cracking methods less effective and allows for users to more easily remember their passwords, reducing the chances of OT members not being able to log in, and the administrative overhead of resetting passwords

CIS Control 17 – Implement a Security Awareness and Training Program	
Introduction	This CIS Control focuses on educating and training the typical enterprise workforce in a range of security practices that span basic to advanced skills to security awareness and vigilance. Human error, oversights, and negligence are leading causes of security weakness, and the consequences of untrained or inadequately, or infrequently trained personnel in an ICS environment and adjacent and interdependent systems can have a range of effects from disruption, damage to destruction of both a digital and physical nature. It is essential for OT teams to be thoroughly versed in security best practices so that they can ensure the security readiness of the ICS environment. These same skills should be nurtured and expanded over time to reinforce best practices and evolve as new risks are identified and new threats emerge. Additionally, many OT teams rely on contractors or vendors who need access to critical parts of the network to service specialized equipment, but they may not be aware of security threats. For these reasons, the experience and pedigree of these third-party resources should be carefully evaluated, including evaluation and validation of purported knowledge, skills, and abilities (KSAs) prior to allowing said third parties access to critical components and systems.
Applicability	Sub-Controls addressing the organizational workforce and testing employee awareness levels through phishing exercises are not applicable.
Considerations	For this CIS Control consider the following additional steps: a. Implement a security awareness program that is mandated for completion by all visitors (Including 3rd parties: contractors, subcontractors, vendors, etc.) prior to granting remote or on-premises site access. b. Consider awareness training that utilizes ICS relevant examples which are relevant to personnel interfacing with ICS. c. Consider background checks and police verification and validation of credentials, experience, and certifications prior to third-party access to critical systems. d. Consider baseline physical and cybersecurity security education to standardize knowledge, skills, and abilities (KSAs) for ICS personnel, as well as others that interface with and support ICS (e.g. IT personnel, IT-OT Hybrid personnel, third-party contractors, service/support personnel, and others as appropriate). e. Consider advanced immersive cybersecurity security education and training for personnel expected to perform f. higher-risk, more advanced processes, or those who are making decisions relating to design, build, operation, and maintenance factors.

Implementation Guidelines	a. Deploy a mechanism for testing/ simulating users and their responses to phishing attacks b. Ensure that training and awareness is delivered contextual to user role, contextual to situation, and based on behaviour demonstrated by the user
CIS Control 18 – Application Software Security	
Introduction	This control focuses on the application security in the OT environment, where countless off-the-shelf, web-based, and proprietary applications can be running on a network. This can be a big task for system administrators. It is not uncommon for ICS environments to contain some custom-engineered, in-house built web-based, or other application software that is specialized for the given system. Such applications and services may not always follow a disciplined engineering development, test, and maintenance process. This can lead to application vulnerabilities that can be exploited by an attacker to aid in gaining access to or pivoting through ICS systems and network architectures. If an environment does contain this software, then this entire Control can be applied with minor modifications. This CIS Control is relevant to ICS environments if they contain web-based or other application software built by OT teams, and aspects of this Control even apply to commercial-off-the-shelf software sourced from product and solution vendors.
Applicability	All the sub-controls are applicable although sub-controls related to automated scanning may not be appropriate.
Considerations	In terms of firewalls, the goal is to protect the web applications when accessible from a lower security zone. Be sure to test in-house-developed and third-party-procured web applications for common security weaknesses using automated application scanners during scheduled maintenance when performance of these applications won't negatively affect the process. Monitoring for the release of software security patches and general product upgrades is an important aspect of maintaining software security. However, retesting after the application of said patches and upgrades is critical since it is not uncommon for new services, capabilities, features to be introduced or enabled, or configuration changes or resets to result from applying these patches and upgrades. Obtaining software patches and upgrades from only the most reputable sources and taking care in the secure transfer of these files is necessary to ensure software assurance, product, and system security. Verifying file hashes, or more ideally, making use of digitally signed software, and using only vendor-approved methods and tools to apply updates help with this assurance. Ensuring that the most current and relevant patch or software version is used, avoiding older versions that may contain known or unknown vulnerabilities also add to helping with software assurance.

Implementation Guidelines	a. Set up an application security governance mechanism to ensure that vulnerabilities and weaknesses are timely identified and issues are resolved in timely manner. b. Ensure a mechanism for understanding, mapping, and analysing software composition c. Set up a process for backward tracing of application module, library, and functionalities, including decisions made for security and privacy
CIS Control 19 – Incident Response and Management	
Introduction	This CIS control addresses the processes and steps required to prepare for an incident. Well-defined and implemented incident response plans can allow an enterprise to identify, contain, reduce impacts, and more quickly recover from a cyber incident. This is especially important for organizations where ICS downtime can lead to safety, health, or profitability impacts affecting the company, employees, customers, supply chain partners, community, and other constituents depending on the safe, reliable operation of an organization. Most OT teams are accustomed to performing some aspects of backups of critical systems to mitigate risks of failed components, loss of services, accidental employee actions, or even aspects of natural disasters. However, there is often a gap in the other areas of incident response, such as efficient coordination, chain of command, decision making authority, impact isolation, reporting, data collection, management responsibility, legal protocols, and communications strategy. Furthermore, it is not unusual for such processes to not be adequately or periodically tested, let alone evolve over time as new variables emerge, risks are identified, and threats evolve.
Applicability	All the Sub-Controls are applicable.

Considerations	For this CIS Control consider the following additional steps: a. If extending an IT Incident Response plan, ensure the Incident Response Plan has been reviewed and approved by ICS Operational Leadership. b. Response teams should be thoroughly familiar with the risks inherent to the ICS environment and mitigations to prevent secondary damage that may impact operational safety and protection of personnel, equipment, information, and a myriad of other dependent and interdependent factors. Aspects of this Control can mimic plans and procedures from non-ICS environments. However, it is not uncommon for these plans to require an augmentation of IT plans and procedures already in place for an enterprises Information technology system in order to be relevant, applicable, and complete for OT.
Implementation Guidelines	Ensure that playbooks for all critical possible incident scenarios are documented and response mechanism is configured to bring systematization and predictability in the response.
CIS Control 20 – Penetration Tests and Red Team Exercises	
Introduction	This CIS Control is focused on designing and conducting controlled penetration testing in an operational technology environment, including connected devices and systems that may not be normally viewed as a constituent component, service, or system for an ICS. The goal is to test both employee responsiveness and the resiliency of internal controls. It refers to conducting tests on connected products, systems, and other interconnected products and systems in a real-time manner to identify, isolate, and demonstrate exploitability of a weakness or vulnerability in the security posture of the ICS. Processes controlled by ICS environments are easily disrupted by penetration testing, red team exercises, or other similar activity. Performing these activities on production systems, even during scheduled outages, can lead to downtime, destruction, injury, or introduce lingering artifacts that reduce the safety, efficiency, or performance of the tested system. For these reasons, it is highly recommended to only perform penetration testing and red-team exercises on non-production systems such as lab equipment, during scheduled-downtime, or during factory acceptance testing when proper oversights and precautions before a system is installed. However, such testing should be conducted periodically since system configurations change, new vulnerabilities are discovered, new threats emerge, and as tools and testing methodologies evolve. When analyzing production systems, it is recommended to use security assessments that are non-intrusive. These assessments can be paper based, utilize passive enumeration of system and network details, or any other activity that does not impact the safety, availability and performance of the ICS environment.

Applicability	Sub-Controls related to penetration tests or red team exercises on production systems do not apply. These Sub-Controls do apply when applied to testing on test bed or non-production systems.
Considerations	Instead of exclusively relying on an internal OT team, also consider conducting regular non-intrusive security assessments with the assistance of third-parties to identify a greater diversity of vulnerabilities and attack vectors that can be used to breach security of ICS systems. Ensure that personnel conducting vulnerability assessments are skilled in working within ICS environments to reduce the possibility of inadvertent negative impact to operations. Careful consideration should be given to the training, experience level, and pedigree of those performing such assessments. Include tests for the presence of unprotected system information, data leakage, and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, documents containing passwords, or other information critical to system operation. Consider using results from vulnerability scans and security assessments in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus security testing efforts. Furthermore, these results should operate as a guide for developing and applying corrective measures and other compensating controls to mitigate risks and better safeguard systems from threats. Personal and functional safety, as well as protecting digital and physical assets throughout the testing process is paramount. Testing an ICS environment's security.
Implementation Guidelines	Incorporate breach simulation, adversarial emulation, threat hunting, and attack surface management to test the strength of security preparedness.

Annexure C

Mapping of Controls (CIS v8-IT v/s ISO/IEC 27001:2022)

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
1		**Inventory and Control of Enterprise Assets**						
1	1.1	Establish and Maintain Detailed Enterprise Asset Inventory	X	X	X	Subset	A5.9	Inventory of information and other associated assets
1	1.1	Establish and Maintain Detailed Enterprise Asset Inventory	X	X	X	Subset	A8.8	Management of technical vulnerabilities
1	1.2	Address Unauthorized Assets	X	X	X			
1	1.3	Utilize an Active Discovery Tool		X	X			
1	1.4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory		X	X			
1	1.5	Use a Passive Asset Discovery Tool			X			
2		**Inventory and Control of Software Assets**						
2	2.1	Establish and Maintain a Software Inventory	X	X	X	Subset	A5.9	Inventory of information and other associated assets
2	2.2	Ensure Authorized Software is Currently Supported	X	X	X			

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
2	2.3	Address Unauthorized Software	X	X	X			
2	2.4	Utilize Automated Software Inventory Tools		X	X			
2	2.5	Allow list Authorized Software		X	X	Subset	A8.7	Protection against malware
2	2.5	Allow list Authorized Software		X	X	Subset	A8.19	Installation of software on operational systems
2	2.6	Allow list Authorized Libraries		X	X	Subset	A8.19	Installation of software on operational systems
2	2.7	Allow list Authorized Scripts			X			
3		**Data Protection**						
3	3.1	Establish and Maintain a Data Management Process	X	X	X	Subset	A5.10	Acceptable use of information and other associated assets
3	3.1	Establish and Maintain a Data Management Process	X	X	X	Subset	A5.9	Inventory of information and other associated assets
3	3.1	Establish and Maintain a Data Management Process	X	X	X	Subset	A8.1	User endpoint devices

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
3	3.2	Establish and Maintain a Data Inventory	X	X	X	Subset	A5.9	Inventory of information and other associated assets
3	3.3	Configure Data Access Control Lists	X	X	X	Subset	A5.10	Acceptable use of information and other associated assets
3	3.3	Configure Data Access Control Lists	X	X	X	Subset	A5.15	Access control
3	3.3	Configure Data Access Control Lists	X	X	X	Subset	A8.3	Information access restriction
3	3.3	Configure Data Access Control Lists	X	X	X	Subset	A8.4	Access to source code
3	3.4	Enforce Data Retention	X	X	X	Subset	A5.33	Protection of records
3	3.5	Securely Dispose of Data	X	X	X	Subset	A5.10	Acceptable use of information and other associated assets
3	3.6	Encrypt Data on End-User Devices	X	X	X	Subset	A6.7	Remote working

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
3	3.6	Encrypt Data on End-User Devices	X	X	X	Subset	A8.1	User endpoint devices
3	3.7	Establish and Maintain a Data Classification Scheme		X	X	Subset	A5.9	Inventory of information and other associated assets
3	3.7	Establish and Maintain a Data Classification Scheme		X	X	Subset	A5.12	Classification of information
3	3.7	Establish and Maintain a Data Classification Scheme		X	X	Subset	A5.13	Labelling of information
3	3.7	Establish and Maintain a Data Classification Scheme		X	X	Subset	A5.33	Protection of records
3	3.7	Establish and Maintain a Data Classification Scheme		X	X	Subset	A8.12	Data leakage prevention
3	3.8	Document Data Flows		X	X	Subset	A5.14	Information transfer
3	3.9	Encrypt Data on Removable Media		X	X	Subset	A5.14	Information transfer

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
3	3.1	Encrypt Sensitive Data in Transit		X	X	Subset	A5.14	Information transfer
3	3.11	Encrypt Sensitive Data at Rest		X	X	Subset	A5.33	Protection of records
3	3.12	Segment Data Processing and Storage Based on Sensitivity		X	X	Subset	A8.20	Networks security
3	3.12	Segment Data Processing and Storage Based on Sensitivity		X	X	Subset	A8.22	Segregation of networks
3	3.13	Deploy a Data Loss Prevention Solution			X	Subset	A5.14	Information transfer
3	3.13	Deploy a Data Loss Prevention Solution			X	Subset	A8.12	Data leakage prevention
3	3.14	Log Sensitive Data Access			X	Subset	A8.15	Logging
4		**Secure Configuration of Enterprise Assets and Software**						
4	4.1	Establish and Maintain a Secure Configuration Process	X	X	X	Subset	A8.1	User endpoint devices

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
4	4.1	Establish and Maintain a Secure Configuration Process	X	X	X	Subset	A8.9	Configuration management
4	4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	X	X	X	Subset	A8.9	Configuration management
4	4.3	Configure Automatic Session Locking on Enterprise Assets	X	X	X	Subset	A8.5	Secure authentication
4	4.3	Configure Automatic Session Locking on Enterprise Assets	X	X	X	Subset	A8.9	Configuration management
4	4.4	Implement and Manage a Firewall on Servers	X	X	X			
4	4.5	Implement and Manage a Firewall on End-User Devices	X	X	X	Subset	A6.7	Remote working
4	4.5	Implement and Manage a Firewall on End-User Devices	X	X	X	Subset	A8.1	User endpoint devices
4	4.6	Securely Manage Enterprise Assets and Software	X	X	X			

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
4	4.7	Manage Default Accounts on Enterprise Assets and Software	X	X	X	Subset	A8.2	Privileged access rights
4	4.7	Manage Default Accounts on Enterprise Assets and Software	X	X	X	Subset	A8.9	Configuration management
4	4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software		X	X	Subset	A8.9	Configuration management
4	4.9	Configure Trusted DNS Servers on Enterprise Assets		X	X			
4	4.1	Enforce Automatic Device Lockout on Portable End-User Devices		X	X	Subset	A8.5	Secure authentication
4	4.11	Enforce Remote Wipe Capability on Portable End-User Devices		X	X	Subset	A8.1	User endpoint devices
4	4.11	Enforce Remote Wipe Capability on Portable End-User Devices		X	X	Subset	A8.10	Information Deletion
4	4.12	Separate Enterprise Workspaces on Mobile End-User Devices			X	Subset	A6.7	Remote working

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
4	4.12	Separate Enterprise Workspaces on Mobile End-User Devices			X	Subset	A8.1	User endpoint devices
5		**Account Management**						
5	5.1	Establish and Maintain an Inventory of Accounts	X	X	X	Subset	A5.16	Identity management
5	5.2	Use Unique Passwords	X	X	X	Subset	A5.17	Authentication information
5	5.3	Disable Dormant Accounts	X	X	X			
5	5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	X	X	X	Subset	A5.15	Access control
5	5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	X	X	X	Subset	A8.2	Privileged access rights
5	5.5	Establish and Maintain an Inventory of Service Accounts		X	X	Subset	A5.15	Access control
5	5.5	Establish and Maintain an Inventory of Service Accounts		X	X	Subset	A8.18	Use of privileged utility programs

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
5	5.6	Centralize Account Management		X	X	Subset	A5.15	Access control
6		**Access Control Management**						
6	6.1	Establish an Access Granting Process	X	X	X	Subset	A5.15	Access control
6	6.1	Establish an Access Granting Process	X	X	X	Subset	A5.16	Identity management
6	6.1	Establish an Access Granting Process	X	X	X	Subset	A5.18	Access rights
6	6.2	Establish an Access Granting Process	X	X	X	Subset	A5.16	Identity management
6	6.2	Establish an Access Granting Process	X	X	X	Subset	A5.18	Access rights
6	6.2	Establish an Access Granting Process	X	X	X	Subset	A6.5	Responsibilities after termination or change of employment

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
6	6.3	Require MFA for Externally-Exposed Applications	X	X	X	Subset	A5.15	Access control
6	6.4	Require MFA for Remote Network Access	X	X	X	Subset	A6.7	Remote working
6	6.5	Require MFA for Administrative Access	X	X	X	Subset	A8.2	Privileged access rights
6	6.6	Establish and Maintain an Inventory of Authentication and Authorization Systems		X	X	Subset	A8.5	Secure authentication
6	6.7	Centralize Access Control		X	X	Subset	A5.18	Access rights
6	6.8	Define and Maintain Role-Based Access Control			X	Superset	A5.3	Segregation of duties
6	6.8	Define and Maintain Role-Based Access Control			X	Subset	A5.15	Access control
6	6.8	Define and Maintain Role-Based Access Control			X	Subset	A8.2	Privileged access rights

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
6	6.8	Define and Maintain Role-Based Access Control			X	Subset	A8.3	Information access restriction
7		**Continuous Vulnerability Management**						
7	7.1	Establish and Maintain a Vulnerability Management Process	X	X	X	Subset	A8.8	Management of technical vulnerabilities
7	7.2	Establish and Maintain a Remediation Process	X	X	X	Subset	A8.8	Management of technical vulnerabilities
7	7.3	Perform Automated Operating System Patch Management	X	X	X	Subset	A8.8	Management of technical vulnerabilities
7	7.4	Perform Automated Application Patch Management	X	X	X	Subset	A8.8	Management of technical vulnerabilities
7	7.5	Perform Automated Vulnerability Scans of Internal Enterprise Assets		X	X	Subset	A8.8	Management of technical vulnerabilities
7	7.6	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets		X	X	Subset	A8.8	Management of technical vulnerabilities

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
7	7.7	Remediate Detected Vulnerabilities		X	X	Subset	A8.8	Management of technical vulnerabilities
8		**Audit Log Management**						
8	8.1	Establish and Maintain an Audit Log Management Process	X	X	X	Equivalent	A8.15	Logging
8	8.2	Collect Audit Logs	X	X	X	Subset	A8.15	Logging
8	8.2	Collect Audit Logs	X	X	X	Subset	A8.20	Networks security
8	8.3	Ensure Adequate Audit Log Storage	X	X	X	Subset	A8.6	Capacity management
8	8.4	Standardize Time Synchronization		X	X	Equivalent	A8.17	Clock synchronization
8	8.5	Collect Detailed Audit Logs		X	X	Subset	A5.28	Collection of evidence

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
8	8.5	Collect Detailed Audit Logs		X	X	Subset	A8.15	Logging
8	8.6	Collect DNS Query Audit Logs		X	X			
8	8.7	Collect URL Request Audit Logs		X	X			
8	8.8	Collect Command-Line Audit Logs		X	X	Subset	A8.15	Logging
8	8.9	Centralize Audit Logs		X	X			
8	8.1	Retain Audit Logs		X	X	Subset	A5.28	Collection of evidence
8	8.11	Conduct Audit Log Reviews		X	X	Subset	A5.25	Assessment and decision on information security events
8	8.12	Collect Service Provider Logs			X			
9		**Email and Web Browser Protections**						

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
9	9.1	Ensure Use of Only Fully Supported Browsers and Email Clients	X	X	X	Subset	A8.1	User endpoint devices
9	9.2	Use DNS Filtering Services	X	X	X	Subset	A8.23	Web filtering
9	9.3	Maintain and Enforce Network-Based URL Filters		X	X	Subset	A8.7	Protection against malware
9	9.3	Maintain and Enforce Network-Based URL Filters		X	X	Subset	A8.23	Web filtering
9	9.4	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions		X	X			
9	9.5	Implement DMARC		X	X			
9	9.6	Block Unnecessary File Types		X	X			
9	9.7	Deploy and Maintain Email Server Anti-Malware Protections			X	Subset	A8.7	Protection against malware

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
10		**Malware Defenses**						
10	10.1	Deploy and Maintain Anti-Malware Software	X	X	X	Subset	A8.1	User endpoint devices
10	10.1	Deploy and Maintain Anti-Malware Software	X	X	X	Subset	A8.7	Protection against malware
10	10.2	Configure Automatic Anti-Malware Signature Updates	X	X	X	Subset	A8.7	Protection against malware
10	10.3	Disable Autorun and Autoplay for Removable Media	X	X	X			
10	10.4	Configure Automatic Anti-Malware Scanning of Removable Media		X	X	Subset	A8.7	Protection against malware
10	10.5	Enable Anti-Exploitation Features		X	X	Subset	A8.7	Protection against malware
10	10.6	Centrally Manage Anti-Malware Software		X	X	Subset	A8.7	Protection against malware

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
10	10.7	Use Behavior-Based Anti-Malware Software		X	X	Subset	A8.1	User endpoint devices
10	10.7	Use Behavior-Based Anti-Malware Software		X	X	Subset	A8.7	Protection against malware
11		**Data Recovery**						
11	11.1	Establish and Maintain a Data Recovery Process	X	X	X	Subset	A8.13	Information backup
11	11.2	Perform Automated Backups	X	X	X	Subset	A8.13	Information backup
11	11.3	Protect Recovery Data	X	X	X	Subset	A8.12	Data leakage prevention
11	11.3	Protect Recovery Data	X	X	X	Subset	A8.13	Information backup
11	11.4	Establish and Maintain an Isolated Instance of Recovery Data	X	X	X	Subset	A8.13	Information backup
11	11.5	Test Data Recovery		X	X	Subset	A8.13	Information backup

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
12		**Network Infrastructure Management**						
12	12.1	Ensure Network Infrastructure is Up-to-Date	X	X	X			
12	12.2	Establish and Maintain a Secure Network Architecture		X	X	Subset	A8.22	Segregation of networks
12	12.2	Establish and Maintain a Secure Network Architecture		X	X	Subset	A8.27	Secure system architecture and engineering principles
12	12.3	Securely Manage Network Infrastructure		X	X	Subset	A8.20	Networks security
12	12.3	Securely Manage Network Infrastructure		X	X	Subset	A8.21	Security of network services
12	12.4	Establish and Maintain Architecture Diagram(s)		X	X			
12	12.5	Centralize Network Authentication, Authorization, and Auditing (AAA)		X	X			

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
12	12.6	Use of Secure Network Management and Communication Protocols		X	X			
12	12.7	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure		X	X	Subset	A6.7	Remote working
12	12.7	Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure		X	X	Subset	A8.1	User endpoint devices
12	12.8	Establish and Maintain Dedicated Computing Resources for All Administrative Work			X	Subset	A8.2	Privileged access rights
12	12.8	Establish and Maintain Dedicated Computing Resources for All Administrative Work			X	Subset	A8.22	Segregation of networks
13		**Network Monitoring and Defense**						
13	13.1	Centralize Security Event Alerting		X	X	Subset	A8.15	Logging
13	13.2	Deploy a Host-Based Intrusion Detection Solution		X	X	Subset	A8.16	Monitoring activities
13	13.3	Deploy a Network Intrusion Detection Solution		X	X	Subset	A8.16	Monitoring activities

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
13	13.4	Perform Traffic Filtering Between Network Segments		X	X	Subset	A8.16	Monitoring activities
13	13.4	Perform Traffic Filtering Between Network Segments		X	X	Subset	A8.22	Segregation of networks
13	13.5	Manage Access Control for Remote Assets		X	X	Subset	A6.7	Remote working
13	13.5	Manage Access Control for Remote Assets		X	X	Subset	A8.1	User endpoint devices
13	13.5	Manage Access Control for Remote Assets		X	X	Subset	A8.3	Information access restriction
13	13.6	Collect Network Traffic Flow Logs		X	X	Subset	A8.15	Logging
13	13.6	Collect Network Traffic Flow Logs		X	X	Subset	A8.16	Monitoring activities
13	13.7	Deploy a Host-Based Intrusion Prevention Solution			X	Subset	A8.8	Management of Technical Vulnerabilities

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
13	13.8	Deploy a Network Intrusion Prevention Solution			X	Subset	A8.8	Management of Technical Vulnerabilities
13	13.9	Deploy Port-Level Access Control			X	Subset	A8.8	Management of Technical Vulnerabilities
13	13.1	Perform Application Layer Filtering			X	Subset	A8.8	Management of Technical Vulnerabilities
13	13.11	Tune Security Event Alerting Thresholds			X			
14		**Security Awareness and Skills Training**						
14	14.1	Establish and Maintain a Security Awareness Program	X	X	X	Subset	A6.3	Information security awareness, education and training
14	14.2	Train Workforce Members to Recognize Social Engineering Attacks	X	X	X	Subset	A8.7	Protection against malware
14	14.3	Train Workforce Members on Authentication Best Practices	X	X	X			
14	14.4	Train Workforce on Data Handling Best Practices	X	X	X	Subset	A5.10	Acceptable use of information and other associated assets

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
14	14.5	Train Workforce Members on Causes of Unintentional Data Exposure	X	X	X	Subset	A6.3	Information security awareness, education and training
14	14.6	Train Workforce Members on Recognizing and Reporting Security Incidents	X	X	X	Subset	A6.3	Information security awareness, education and training
14	14.6	Train Workforce Members on Recognizing and Reporting Security Incidents	X	X	X	Subset	A6.8	Information security event reporting
14	14.7	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	X	X	X	Subset	A6.3	Information security awareness, education and training
14	14.8	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	X	X	X	Subset	A6.3	Information security awareness, education and training
14	14.9	Conduct Role-Specific Security Awareness and Skills Training		X	X	Subset	A6.3	Information security awareness, education and training
15		**Service Provider Management**						
15	15.1	Establish and Maintain an Inventory of Service Providers	X	X	X	Subset	A5.19	Information security in supplier relationships

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
15	15.2	Establish and Maintain a Service Provider Management Policy		X	X	Subset	A5.1	Policies for information security
15	15.2	Establish and Maintain a Service Provider Management Policy		X	X	Subset	A5.10	Acceptable use of information and other associated assets
15	15.2	Establish and Maintain a Service Provider Management Policy		X	X	Subset	A5.10	Acceptable use of information and other associated assets
15	15.2	Establish and Maintain a Service Provider Management Policy		X	X	Subset	A5.19	Information security in supplier relationships
15	15.2	Establish and Maintain a Service Provider Management Policy		X	X	Subset	A5.20	Addressing information security within supplier agreements
15	15.2	Establish and Maintain a Service Provider Management Policy		X	X	Subset	A5.23	Information security for use of cloud services
15	15.3	Classify Service Providers		X	X	Subset	A5.19	Information security in supplier relationships
15	15.4	Ensure Service Provider Contracts Include Security Requirements		X	X	Subset	A5.14	Information transfer

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
15	15.4	Ensure Service Provider Contracts Include Security Requirements		X	X	Subset	A5.20	Addressing information security within supplier agreements
15	15.4	Ensure Service Provider Contracts Include Security Requirements		X	X	Subset	A5.21	Managing information security in the ICT supply chain
15	15.4	Ensure Service Provider Contracts Include Security Requirements		X	X	Subset	A5.23	Information security for use of cloud services
15	15.5	Assess Service Providers			X	Subset	A5.19	Information security in supplier relationships
15	15.5	Assess Service Providers			X	Subset	A5.22	Monitoring, review and change management of supplier services
15	15.5	Assess Service Providers			X	Subset	A5.23	Information security for use of cloud services
15	15.6	Monitor Service Providers			X	Subset	A5.19	Information security in supplier relationships
15	15.6	Monitor Service Providers			X	Subset	A5.20	Addressing information security within supplier agreements

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
15	15.6	Monitor Service Providers			X	Subset	A5.22	Monitoring, review and change management of supplier services
15	15.6	Monitor Service Providers			X	Subset	A5.21	Managing information security in the ICT supply chain
15	15.7	Securely Decommission Service Providers			X	Subset	A5.19	Information security in supplier relationships
15	15.7	Securely Decommission Service Providers			X	Subset	A5.20	Addressing information security within supplier agreements
16		**Application Software Security**						
16	16.1	Establish and Maintain a Secure Application Development Process		X	X	Subset	A5.8	Information security in project management
16	16.1	Establish and Maintain a Secure Application Development Process		X	X	Superset	A8.4	Access to source code
16	16.1	Establish and Maintain a Secure Application Development Process		X	X	Superset	A8.25	Secure development life cycle
16	16.1	Establish and Maintain a Secure Application Development Process		X	X	Superset	A8.28	Secure coding

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
16	16.2	Establish and Maintain a Process to Accept and Address Software Vulnerabilities		X	X	Subset	A8.8	Management of Technical vulnerabilities
16	16.3	Perform Root Cause Analysis on Security Vulnerabilities		X	X	Subset	A8.8	Management of Technical vulnerabilities
16	16.4	Establish and Manage an Inventory of Third-Party Software Components		X	X	Subset	A8.26	Application security requirements
16	16.4	Establish and Manage an Inventory of Third-Party Software Components		X	X	Subset	A8.30	Outsourced development
16	16.5	Use Up-to-Date and Trusted Third-Party Software Components		X	X	Subset	A8.26	Application security requirements
16	16.6	Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities		X	X	Subset	A8.8	Management of Technical vulnerabilities
16	16.7	Use Standard Hardening Configuration Templates for Application Infrastructure		X	X	Subset	A8.8	Management of Technical vulnerabilities
16	16.8	Separate Production and Non-Production Systems		X	X	Equivalent	A8.31	Separation of development, test and production

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
16	16.9	Train Developers in Application Security Concepts and Secure Coding		X	X	Subset	A8.28	Secure coding
16	16.1	Apply Secure Design Principles in Application Architectures		X	X	Subset	A8.27	Secure system architecture and engineering principles
16	16.11	Leverage Vetted Modules or Services for Application Security Components		X	X	Subset	A8.25	Secure development life cycle
16	16.11	Leverage Vetted Modules or Services for Application Security Components		X	X	Subset	A8.26	Application security requirements
16	16.12	Implement Code-Level Security Checks			X	Subset	A8.25	Secure development life cycle
16	16.12	Implement Code-Level Security Checks			X	Subset	A8.28	Secure coding
16	16.12	Implement Code-Level Security Checks			X	Subset	A8.29	Security testing in development and acceptance
16	16.13	Conduct Application Penetration Testing			X	Subset	A8.8	Management of Technical vulnerabilities

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
16	16.13	Conduct Application Penetration Testing			X	Subset	A8.29	Security testing in development and acceptance
16	16.14	Conduct Threat Modeling			X	Subset	A8.29	Security testing in development and acceptance
17		**Incident Response Management**						
17	17.1	Designate Personnel to Manage Incident Handling	X	X	X	Subset	A5.24	Information security incident management planning and
17	17.2	Establish and Maintain Contact Information for Reporting Security Incidents	X	X	X	Superset	A5.5	Contact with authorities
17	17.2	Establish and Maintain Contact Information for Reporting Security Incidents	X	X	X	Subset	A5.6	Contact with special interest groups
17	17.2	Establish and Maintain Contact Information for Reporting Security Incidents	X	X	X	Subset	A5.20	Addressing information security within supplier agreements
17	17.2	Establish and Maintain Contact Information for Reporting Security Incidents	X	X	X	Subset	A5.24	Information security incident management planning and
17	17.3	Establish and Maintain an Enterprise Process for Reporting Incidents	X	X	X	Equivalent	A6.8	Information security event reporting

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
17	17.4	Establish and Maintain an Incident Response Process		X	X	Subset	A5.24	Information security incident management planning and
17	17.4	Establish and Maintain an Incident Response Process		X	X	Subset	A5.26	Response to information security incidents
17	17.5	Assign Key Roles and Responsibilities		X	X	Subset	A5.2	Information security roles and responsibilities
17	17.5	Assign Key Roles and Responsibilities		X	X	Subset	A5.24	Information security incident management planning and
17	17.6	Define Mechanisms for Communicating During Incident Response		X	X	Subset	A5.24	Information security incident management planning and
17	17.7	Conduct Routine Incident Response Exercises		X	X	Subset	A5.30	ICT readiness for business continuity
17	17.8	Conduct Post-Incident Reviews		X	X	Subset	A5.24	Information security incident management planning and
17	17.8	Conduct Post-Incident Reviews		X	X	Subset	A5.27	Learning from information security incidents

CIS Control	CIS Safeguard	Title	IG1	IG2	IG3	Relationship	Control (ISO 27001:2022)	Control Title
17	17.9	Establish and Maintain Security Incident Thresholds			X	Subset	A5.24	Information security incident management planning and
17	17.9	Establish and Maintain Security Incident Thresholds			X	Subset	A5.25	Assessment and decision on information security events
18		**Penetration Testing**						
18	18.1	Establish and Maintain a Penetration Testing Program		X	X	Subset	A8.8	Management of Technical vulnerabilities
18	18.2	Perform Periodic External Penetration Tests		X	X	Subset	A8.8	Management of Technical vulnerabilities
18	18.3	Remediate Penetration Test Findings		X	X	Subset	A8.8	Management of Technical vulnerabilities
18	18.4	Validate Security Measures			X	Subset	A8.8	Management of Technical vulnerabilities
18	18.5	Perform Periodic Internal Penetration Tests			X	Subset	A8.8	Management of Technical vulnerabilities

Annexure D

Mapping of Controls (CIS v7.1-ICS v/s ISO/IEC 27001:2022)

Note: This is adopted from version 'v 7/v 7.1 CIS Controls: Implementation Guide for Industrial Control Systems' available at www.cisecurity.org

CIS Control	CIS Sub-Control	Title	Description	Relationship	ISO 27001 Objective Number
1		**Inventory and Control of Hardware Assets**			
		Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.			

1	1.1	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.	small subset	A.8.1.1
1	1.2	Use a Passive Asset Discovery Tool	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.	small subset	A.8.1.1
1	1.3	Use DHCP Logging to Update Asset Inventory	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.	small subset	**A.8.1.1**
1	1.4	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.	large subset	A.8.1.1

1	1.5	Maintain Asset Inventory Information	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.	small subset	A.8.1.1
1	1.6	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.	small subset	A.11.2.5
1	1.7	Deploy Port Level Access Control	Utilize port-level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure that only authorized devices can connect to the network.	small subset	A.13.1.1
				large subset	A.9.1.2
1	1.8	Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.	small subset	A.9.3.1
1	1.8	Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.	small subset	A.13.1.1
2		**Inventory and Control of Software Assets**			
		Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.			

2	2.1	Maintain Inventory of Authorized Software	Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.	large subset	A.8.1.1
2	2.2	Ensure Software is Supported by Vendor	Ensure that only software applications or operating systems currently supported by the software vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.		
2	2.3	Utilize Software Inventory Tools	Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.		
2	2.4	Track Software Inventory Information	The software inventory system should track the name, version, publisher, and install date for all software, including operating systems authorized by the organization.	small subset	A.8.1.1
2	2.5	Integrate Software and Hardware Asset Inventories	The software inventory system should be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.		
2	2.6	Address unapproved software	Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	small subset	A.12.5.1
				small subset	A.12.6.2
2	2.7	Utilize Application Whitelisting	Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.		

2	2.8	Implement Application Whitelisting of Libraries	The organization's application whitelisting software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc.) are allowed to load into a system process.		
2	2.9	Implement Application Whitelisting of Scripts	The organization's application whitelisting software must ensure that only authorized, digitally signed scripts (such as *.ps1, *.py, macros, etc.) are allowed to run on a system.		
2	2.10	Physically or Logically Segregate High Risk Applications	Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incur higher risk for the organization.		
3		**Continuous Vulnerability Management**			
		Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.			
3	3.1	Run Automated Vulnerability Scanning Tools	Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		
3	3.2	Perform Authenticated Vulnerability Scanning	Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.		

3	3.3	Protect Dedicated Assessment Accounts	Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.		
3	3.4	Deploy Automated Operating System Patch Management Tools	Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.		
3	3.5	Deploy Automated Software Patch Management Tools	Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.		
3	3.6	Compare Back-to-back Vulnerability Scans	Regularly compare the results from back-to-back vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.		
3	3.7	Utilize a Risk-rating Process	Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.	small subset	A.12.6.1
4		**Controlled Use of Administrative Privileges**			
		The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.			
4	4.1	Maintain Inventory of Administrative Accounts	Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		

4	4.2	Change Default Passwords	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	small subset	A.9.4.3
4	4.3	Ensure the Use of Dedicated Administrative Accounts	Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	small subset	A.9.2.3
4	4.4	Use Unique Passwords	Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.	large subset	A.9.4.3
4	4.5	Use Multifactor Authentication For All Administrative Access	Use multi-factor authentication and encrypted channels for all administrative account access.		
4	4.6	Use of Dedicated Machines For All Administrative Tasks	Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.		
4	4.7	Limit Access to Script Tools	Limit access to scripting tools (such as Microsoft PowerShell and Python) to only administrative or development users with the need to access those capabilities.		

4	4.8	Log and Alert on Changes to Administrative Group Membership	Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.	small subset	A.12.4.3
4	4.9	Log and Alert on Unsuccessful Administrative Account Login	Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.	small subset	A.9.4.2
5		**Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers**			
		Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.			
5	5.1	Establish Secure Configurations	Maintain documented, standard security configuration standards for all authorized operating systems and software.	large subset	A.8.1.3
				small subset	A.14.2.5
5	5.2	Maintain Secure Images	Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.		
5	5.3	Securely Store Master Images	Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.		

5	5.4	Deploy System Configuration Management Tools	Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.		
5	5.5	Implement Automated Configuration Monitoring Systems	Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.		
6		**Maintenance, Monitoring and Analysis of Audit Logs**			
		Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.			
6	6.1	Utilize Three Synchronized Time Sources	Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.	large subset	A.12.4.4
6	6.2	Activate audit logging	Ensure that local logging has been enabled on all systems and networking devices.	large subset	A.12.4.1
6	6.3	Enable Detailed Logging	Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		
6	6.4	Ensure adequate storage for logs	Ensure that all systems that store logs have adequate storage space for the logs generated.		

6	6.5	Central Log Management	Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		
6	6.6	Deploy SIEM or Log Analytic tool	Deploy Security Information and Event Management (SIEM) or log analytic tool for log correlation and analysis.		
6	6.7	Regularly Review Logs	On a regular basis, review logs to identify anomalies or abnormal events.	small superset	A.12.4.3
6	6.8	Regularly Tune SIEM	On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.		
7		**Email and Web Browser Protections**			
		Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.			
7	7.1	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.	small subset	A.8.1.3
7	7.2	Disable Unnecessary or Unauthorized Browser or Email Client Plugins	Uninstall or disable any unauthorized browser or email client plugins or add-on applications.	small subset	A.12.6.2
7	7.3	Limit Use of Scripting Languages in Web Browsers and Email Clients	Ensure that only authorized scripting languages are able to run in all web browsers and email clients.		

7	7.4	Maintain and Enforce Network-Based URL Filters	Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.	small subset	A.13.1.1
7	7.5	Subscribe to URL-Categorization Service	Subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.		
7	7.6	Log all URL requester	Log all URL requests from each of the organization's systems, whether on-site or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.		
7	7.7	Use of DNS Filtering Services	Use DNS filtering services to help block access to known malicious domains.	small subset	A.13.1.1
				small subset	A.12.2.1
7	7.8	Implement DMARC and Enable Receiver-Side Verification	To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification, starting by implementing the Sender Policy Framework (SPF) and the Domain Keys Identified Mail(DKIM) standards.	small subset	A.13.2.3
7	7.9	Block Unnecessary File Types	Block all e-mail attachments entering the organization's email gateway if the file types are unnecessary for the organization's business.	small subset	A.13.1.1

7	7.10	Sandbox All Email Attachments	Use sandboxing to analyze and block inbound email attachments with malicious behavior.	small subset	A.12.2.1
8		**Malware Defenses**			
		Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.			
8	8.1	Utilize Centrally Managed Anti-malware Software	Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.	small subset	A.12.2.1
8	8.2	Ensure Anti-Malware Software and Signatures are Updated	Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.	small subset	A.12.2.1
8	8.3	Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies	Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		
8	8.4	Configure Anti-Malware Scanning of Removable Devices	Configure devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected.	small subset	A.12.2.1
8	8.5	Configure Devices Not To Auto-Run Content	Configure devices to not auto-run content from removable media.	small subset	A.12.2.1
8	8.6	Centralize Anti-Malware Logging	Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.	small subset	A.12.4.1
				small subset	A.12.2.1

8	8.7	Enable DNS Query Logging	Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.	small subset	A.12.4.1
8	8.8	Enable Command-Line Audit Logging	Enable command-line audit logging for command shells, such as Microsoft PowerShell and Bash.	small subset	A.12.14.1
9		**Limitation and Control of Network Ports, Protocols, and Services** ***Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.***			
9	9.1	Associate Active Ports, Services and Protocols to Asset Inventory	Associate active ports, services and protocols to the hardware assets in the asset inventory.	small subset	A.13.1.2
9	9.2	Ensure Only Approved Ports, Protocols and Services Are Running	Ensure that only network ports, protocols, and services listening on a system with validated business needs are running on each system.	small subset	A.13.1.3
9	9.3	Perform Regular Automated Port Scans	Perform automated port scans on a regular basis against all systems and alert if unauthorized ports are detected on a system.	small subset	A.13.1.1
9	9.4	Apply Host-Based Firewalls or Port Filtering	Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	small subset	A.13.1.1
9	9.5	Implement Application Firewalls	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.		

10		**Data Recovery Capabilities**			
		The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.			
10	10.1	Ensure Regular Automated BackUps	Ensure that all system data is automatically backed up on a regular basis.	large subset	A.12.3.1
10	10.2	Perform Complete System Backups	Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.		
10	10.3	Test Data on Backup Media	Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.	large subset	A.12.3.1
10	10.4	Ensure Protection of Backups	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.		
10	10.5	Ensure Backups Have At least One Non-Continuously Addressable Destination	Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.		
11		**Secure Configuration for Network Devices, such as Firewalls, Routers and Switches**			
		Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.			

11	11.1	Maintain Standard Security Configurations for Network Devices	Maintain standard, documented security configuration standards for all authorized network devices.		
11	11.2	Document Traffic Configuration Rules	All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		
11	11.3	Use Automated Tools to Verify Standard Device Configurations and Detect Changes	Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.	small subset	A.12.1.2
11	11.4	Install the Latest Stable Version of Any Security-Related Updates on All Network Devices	Install the latest stable version of any security-related updates on all network devices.		
11	11.5	Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions	Manage all network devices using multi-factor authentication and encrypted sessions.		
11	11.6	Use Dedicated Machines For All Network Administrative Tasks	Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.		

11	11.7	Manage Network Infrastructure Through a Dedicated Network	Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.	small subset	A.13.1.3
12		**Boundary Defense**			
		Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.			
12	12.1	Maintain an Inventory of Network Boundaries	Maintain an up-to-date inventory of all of the organization's network boundaries.		
12	12.2	Scan for Unauthorized Connections across Trusted Network Boundaries	Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.	small subset	A.13.1.1
12	12.3	Deny Communications with Known Malicious IP Addresses	Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries,.	small subset	A.13.1.1
12	12.4	Deny Communication over Unauthorized Ports	Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.	small subset	A.13.1.1

12	12.5	Configure Monitoring Systems to Record Network Packets	Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.		
12	12.6	Deploy Network-Based IDS Sensors	Deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the organization's network boundaries.	small subset	A.13.1.1
12	12.7	Deploy Network-Based Intrusion Prevention Systems	Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.	small subset	A.13.1.1
12	12.8	Deploy NetFlow Collection on Networking Boundary Devices	Enable the collection of NetFlow and logging data on all network boundary devices.	small subset	A.13.1.1
12	12.9	Deploy Application Layer Filtering Proxy Server	Ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy that is configured to filter unauthorized connections.	small subset	A.13.1.1
12	12.10	Decrypt Network Traffic at Proxy	Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.		
12	12.11	Require All Remote Login to Use Multi-Factor Authentication	Require all remote login access to the organization's network to encrypt data in transit and use multi-factor authentication.	small subset	A.9.4.2

12	12.12	Manage All Devices Remotely Logging into Internal Network	Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.	small subset	A.9.4.2
13		**Data Protection**			
		The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.			
13	13.1	Maintain an Inventory of Sensitive Information	Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider.	equal	A.8.2.1
13	13.2	Remove Sensitive Data or Systems Not Regularly Accessed by Organization	Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.		
13	13.3	Monitor and Block Unauthorized Network Traffic	Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.	small subset	A.13.1.1
13	13.4	Only Allow Access to Authorized Cloud Storage or Email Providers	Only allow access to authorized cloud storage or email providers.	small subset	A.13.2.3

13	13.5	Monitor and Detect Any Unauthorized Use of Encryption	Monitor all traffic leaving the organization and detect any unauthorized use of encryption.	small subset	A.13.1.1
13	13.6	Encrypt the Hard Drive of All Mobile Devices.	Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices.	small subset	A.6.2.1
13	13.7	Manage USB Devices	If USB storage devices are required, enterprise software should be used that can configure systems to allow the use of specific devices. An inventory of such devices should be maintained.	large subset	A.8.3.1
13	13.8	Manage System's External Removable Media's Read/Write Configurations	Configure systems not to write data to external removable media, if there is no business need for supporting such devices.	small subset	A.8.3.1
13	13.9	Encrypt Data on USB Storage Devices	If USB storage devices are required, all data stored on such devices must be encrypted while at rest.	small subset	A.10.1.1
14		**Controlled Access Based on the Need to Know**			
		The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.			
14	14.1	Segment the Network Based on Sensitivity	Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).	small subset	A.13.1.3

14	14.2	Enable Firewall Filtering Between VLANs	Enable firewall filtering between VLANs to ensure that only authorized systems are able to communicate with other systems necessary to fulfill their specific responsibilities.	small subset	A.13.1.1
14	14.3	Disable Workstation to Workstation Communication	Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems, through technologies such as Private VLANs or micro segmentation.	small subset	A.13.1.1
14	14.4	Encrypt All Sensitive Information in Transit	Encrypt all sensitive information in transit.	large superset	A.13.1.1
				large subset	A.10.1.1
14	14.5	Utilize an Active Discovery Tool to Identify Sensitive Data	Utilize an active discovery tool to identify all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located on-site or at a remote service provider, and update the organization's sensitive information inventory.		
14	14.6	Protect Information through Access Control Lists	Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	large subset	A.9.1.1

14	14.7	Enforce Access Control to Data through Automated Tools	Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system.		
14	14.8	Encrypt Sensitive Information at Rest	Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.	large subset	A.10.1.1
14	14.9	Enforce Detail Logging for Access or Changes to Sensitive Data	Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).	small subset	A.12.4.3
15		**Wireless Access Control**			
		The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (WLANs), access points, and wireless client systems.			
15	15.1	Maintain an Inventory of Authorized Wireless Access Points	Maintain an inventory of authorized wireless access points connected to the wired network.	small subset	A.8.1.1
15	15.2	Detect Wireless Access Points Connected to the Wired Network	Configure network vulnerability scanning tools to detect and alert on unauthorized wireless access points connected to the wired network.	small subset	A.13.1.1
15	15.3	Use a Wireless Intrusion Detection System	Use a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network.	small subset	A.13.1.1
15	15.4	Disable Wireless Access on Devices if Not Required	Disable wireless access on devices that do not have a business purpose for wireless access.	small subset	A.8.1.3

15	15.5	Limit Wireless Access on Client Devices	Configure wireless access on client machines that do have an essential wireless business purpose, to allow access only to authorized wireless networks and to restrict access to other wireless networks.	small subset	A.8.1.3
15	15.6	Disable Peer-to-Peer Wireless Network Capabilities on Wireless Clients	Disable peer-to-peer (ad hoc) wireless network capabilities on wireless clients.	small subset	A.8.1.3
15	15.7	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data	Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.	small subset	A.13.1.1
				small subset	A.10.1.1
15	15.8	Use Wireless Authentication Protocols that Require Mutual, Multi-Factor Authentication	Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), which requires mutual, multi-factor authentication.	small subset	A.13.1.1
15	15.9	Disable Wireless Peripheral Access of Devices	Disable wireless peripheral access of devices (such as Bluetooth and NFC), unless such access is required for a business purpose.	small subset	A.8.1.3
15	15.10	Create Separate Wireless Network for Personal and Untrusted Devices	Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.	large subset	A.13.1.3
16		**Account Monitoring and Control**			
		Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.			

16	16.1	Maintain an Inventory of Authentication Systems	Maintain an inventory of each of the organization's authentication systems, including those located on-site or at a remote service provider.	small	A.8.1.1
16	16.2	Configure Centralized Point of Authentication	Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		
16	16.3	Require Multi-Factor Authentication	Require multi-factor authentication for all user accounts, on all systems, whether managed on-site or by a third-party provider.		
16	16.4	Encrypt or Hash all Authentication Credentials	Encrypt or hash with a salt all authentication credentials when stored.	small subset	A.10.1.1
16	16.5	Encrypt Transmittal of Username and Authentication Credentials	Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.	small subset	A.10.1.1
				small subset	A.13.1.1
16	16.6	Maintain an Inventory of Accounts	Maintain an inventory of all accounts organized by authentication system.	small subset	A.9.2.1
16	16.7	Establish Process for Revoking Access	Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.	large subset	A.9.2.6
16	16.8	Disable Any Unassociated Accounts	Disable any account that cannot be associated with a business process or business owner.		
16	16.9	Disable Dormant Accounts	Automatically disable dormant accounts after a set period of inactivity.		

16	16.10	Ensure All Accounts Have An Expiration Date	Ensure that all accounts have an expiration date that is monitored and enforced.		
16	16.11	Lock Workstation Sessions After Inactivity	Automatically lock workstation sessions after a standard period of inactivity.	small subset	A.8.1.3
16	16.12	Monitor Attempts to Access Deactivated Accounts	Monitor attempts to access deactivated accounts through audit logging.		
16	16.13	Alert on Account Login Behaviour Deviation	Alert when users deviate from normal login behaviour, such as time-of-day, workstation location and duration.		
17		**Implement a Security Awareness and Training Program**			
		For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.			
17	17.1	Perform a Skills Gap Analysis	Perform a skills gap analysis to understand the skills and behaviours workforce members are not adhering to, using this information to build a baseline education roadmap.		
17	17.2	Deliver Training to Fill the Skills Gap	Deliver training to address the skills gap identified to positively impact workforce members' security behaviour.	small subset	A.7.2.2

17	17.3	Implement a Security Awareness Program	Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviours and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.	large subset	A.7.2.2
17	17.4	Update Awareness Content Frequently	Ensure that the organization's security awareness program is updated frequently (at least annually) to address new technologies, threats, standards and business requirements.	small subset	A.7.2.2
17	17.5	Train Workforce on Secure Authentication	Train workforce members on the importance of enabling and utilizing secure authentication.	small subset	A.7.2.2
17	17.6	Train Workforce on Identifying Social Engineering Attacks	Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams and impersonation calls.	small subset	A.7.2.2
17	17.7	Train Workforce on Sensitive Data Handling	Train workforce on how to identify and properly store, transfer, archive and destroy sensitive information.	small subset	A.7.2.2
17	17.8	Train Workforce on Causes of Unintentional Data Exposure	Train workforce members to be aware of causes for unintentional data exposures, such as losing their mobile devices or emailing the wrong person due to autocomplete in email.	small subset	A.7.2.2
17	17.9	Train Workforce Members on Identifying and Reporting Incidents	Train employees to be able to identify the most common indicators of an incident and be able to report such an incident.	small subset	A.7.2.2

18		**Application Software Security**			
		Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.			
18	18.1	Establish Secure Coding Practices	Establish secure coding practices appropriate to the programming language and development environment being used.	small subset	A.14.2.1
18	18.2	Ensure Explicit Error Checking is Performed for All In-House Developed Software	For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.		
18	18.3	Verify That Acquired Software is Still Supported	Verify that the version of all software acquired from outside your organization is still supported by the developer or appropriately hardened based on developer security recommendations.		
18	18.4	Only Use Up-to-Date And Trusted Third-Party Components	Only use up-to-date and trusted third-party components for the software developed by the organization.		
18	18.5	Use Only Standardized and Extensively Reviewed Encryption Algorithms	Use only standardized and extensively reviewed encryption algorithms.	small subset	A.10.1.1
18	18.6	Ensure Software Development Personnel are Trained in Secure Coding	Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities.		

18	18.7	Apply Static and Dynamic Code Analysis Tools	Apply static and dynamic analysis tools to verify that secure coding practices are being adhered to for internally developed software.		
18	18.8	Establish a Process to Accept and Address Reports of Software Vulnerabilities	Establish a process to accept and address reports of software vulnerabilities, including providing a means for external entities to contact your security group.		
18	18.9	Separate Production and Non-Production Systems	Maintain separate environments for production and non-production systems. Developers should not have unmonitored access to production environments.	large subset	A.12.1.4
18	18.10	Deploy Web Application Firewalls (WAFs)	Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.		
18	18.11	Use Standard Hardening Configuration Templates for Databases	For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.		
19		**Incident Response and Management**			

		Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.			
19	19.1	Document Incident Response Procedures	Ensure that there are written incident response plans that define roles of personnel as well as phases of incident handling/management.	equal	A.16.1.1
19	19.2	Assign Job Titles and Duties for Incident Response	Assign job titles and duties for handling computer and network incidents to specific individuals and ensure tracking and documentation throughout the incident through resolution.		
19	19.3	Designate Management Personnel to Support Incident Handling	Designate management personnel, as well as backups, who will support the incident handling process by acting in key decision-making roles.		
19	19.4	Devise Organization-wide Standards for Reporting Incidents	Devise organization-wide standards for the time required for system administrators and other workforce members to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.	large subset	A.16.1.3
19	19.5	Maintain Contact Information For Reporting Security Incidents	Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and ISAC partners.	equal	A.6.1.3

19	19.6	Publish Information Regarding Reporting Computer Anomalies and Incidents	Publish information for all workforce members, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities.		
19	19.7	Conduct Periodic Incident Scenario Sessions for Personnel	Plan and conduct routine incident, response exercises and scenarios for the workforce involved in the incident response to maintain awareness and comfort in responding to real world threats. Exercises should test communication channels, decision making, and incident responders technical capabilities using tools and data available to them.		
19	19.8	Create Incident Scoring and Prioritization Schema	Create incident scoring and prioritization schema based on known or potential impact to your organization. Utilize score to define frequency of status updates and escalation procedures.		
20		**Penetration Tests and Red Team Exercises**			
		Test the overall strength of an organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.			
20	20.1	Establish a Penetration Testing Program	Establish a program for penetration tests that includes a full scope of blended attacks, such as wireless, client-based, and web application attacks.		

20	20.2	Conduct Regular External and Internal Penetration Tests	Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.		
20	20.3	Perform Periodic Red Team Exercises	Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.		
20	20.4	Include Tests for Presence of Unprotected System Information and Artifacts	Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords or other information critical to system operation.		
20	20.5	Create Test Bed for Elements Not Typically Tested in Production	Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.		
20	20.6	Use Vulnerability Scanning and Penetration Testing Tools in Concert	Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.		

20	20.7	Ensure Results from Penetration Test are Documented Using Open, Machine-readable Standards	Wherever possible, ensure that Red Team results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.		
20	20.8	Control and Monitor Accounts Associated with Penetration Testing	Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.		

SECTION 4

INSPECTION PROCESS

1. Purpose

This document defines the process to be followed by inspection bodies operating inspection Schemes to carry out testing and assessment of assets/infrastructure of critical sector entities to find out their security posture.

2. Scope

2.1 The scope of the document covers the inspection process for CSEs having IT/ICS components to the requirements covered in the inspection criteria.

2.2 The scope of this document covers activities by which an inspection body determines that a CSE fulfils inspection requirements including application, inspection, review of inspection report, re-inspection, and use of Scheme mark.

3. Objectives

The objectives of this process are to:

3.1 Ensure uniformity in the inspection of CII of CSEs as per inspection criteria defined in the Scheme document. This process will ensure that the inspection reports are reliable and reproducible in nature.

3.2 Ensure adequate control of the audit process is exercised.

4. Roles and Responsibilities of officials of IB

S No.	Role	Responsibility
1.	Head IB	• Overall management of Inspection Body. Formation of the Inspection Team. • Reports to the Board (The designation can be as per the organisation's culture)
2.	Inspection Team Leader	Responsible for the entire inspection process including managing the inspection programme, conducting inspection, inspection reporting, audit follow-up and making the final recommendation in the inspection report regarding the security posture of IT/ICS infrastructure.
3.	Inspectors	Responsible for inspecting as per task assigned by the Team Leader.
4.	Technical Experts	Responsible for advising the Team Leader on technical issues during inspection.
5.	IB Secretariat	Responsible for coordinating activities during all stages of the inspection process and providing necessary support to the inspection team. Also responsible for maintaining inspection Scheme documentation and records.

5. Process

5.1 Application for Inspection

5.1.1 CSEs interested in getting their infrastructure inspected by an inspection body shall submit an application form for inspection along with the following documents:

*Note: It is advised that the applicant CSE shall study the availability of accredited IBs and may choose the body as per their scope preferring the same body which was selected for CSMS audit (*BTC (Level 1), STC (Level 2) and ATC (Level 3)*) for economic reasons.*

a. Policy and Process documents pertaining to the implementation of controls are given in Annex A in Section 3 of Inspection Criteria for IT and Annex B in Section 3 of Inspection Criteria for ICS, as applicable.

b. Roles and responsibilities of the persons responsible for ensuring that IT/ICS system infrastructure is hardened in the organisation and nominating representatives for interaction with IB. This shall include the competencies and skill sets of this role.

c. Deployed System architecture and network drawings

d. Threat modelling procedure and report

e. Access to asset register/database

f. Provide access to documentation pertaining to vendor-specific *controls and settings* for catalogue products used in the infrastructure.

g. Documentation pertaining to organisation *rule base* for internet, communication and computing devices/components based on the design.

h. SoA and description of elements/controls which are commonly implemented with CSMS *(*BTC (Level 1), STC (Level 2) and ATC (Level 3)*)* Register of countermeasures and reference to the risk being mitigated by them.

i. Vulnerability Analysis and Penetration Testing Reports (may be internal)

5.1.2 Scope of inspection

CSEs shall specify the scope of inspection covering the boundaries of complete CII. If any exemptions are sought, reason for the same is documented. The scope shall also cover the remote devices/systems. Along with application, the following shall be submitted:

a. Application Fee
b. Contract Agreement
c. Document Review Report (Cross reference matrix) for IT or ICS or both as per criteria specified in Annex A and/or Annex B of ‘Section 3: Inspection Criteria’.

Note: Document Review Report is the outcome of the process of reviewing for adequacy as per the requirements of inspection criteria. This is done to ensure that the IT/ICS system infrastructure is defined adequately, assets are traceable to deployed architecture (accuracy of assets discovery) and adhering to the clauses as mentioned in

the inspection criteria in the definition. Generally, it is done using Cross Reference Matrix records (CRR) wherein against each clause of the inspection criteria compliance is ensured and a statement to that effect is recorded.

5.1.3 Before applying for inspection, the applicant shall have met the following conditions:

a. Operated internal 'inspection plan' as per the inspection criteria for not older than 6 months. This is necessary to ensure the ability of the applicant to have a stabilised system under normal operating conditions.

b. Carried out a minimum of one vulnerability assessment and one round of penetration testing of complete CII.

c. An executive report of the system hardening shall be submitted to the management. Considerations should be given to the following:

i. CSEs shall have procedures supported by mechanisms for Asset Hardening.

ii. The goal of ICS Asset Hardening is to reduce security risk by eliminating potential attack vectors and condensing the environment's attack surface. By removing unnecessary programs, user accounts, functionality, connectivity, ports, permissions, physical access, etc. malicious attackers, and malware have fewer opportunities to gain a foothold within the ICS environment.

iii. Asset Hardening demands a methodical approach to assess, identify, remove and control potential security vulnerabilities throughout your ICS environment. The ICS Asset Hardening includes:

- Application hardening;
- Server hardening;
- Endpoint hardening;
- Database hardening;
- Network hardening.
- Operating System (OS) hardening;

Note: There exist several industry standards and guidelines for system hardening processes and procedures. The National Institute of Standards and Technology (NIST), the Computer Information Security (CIS) and Center for Internet Security, for example, are well recognised for maintaining standards w.r.t system hardening best practices manuals. For example, system hardening best practices outlined by the NIST in Special Publication (SP) 800-123 include:

a. Establishing a system security plan
b. Patching and updating the OS.
c. Removing or disabling unnecessary services, applications, and network protocols
d. Configuring OS user authentication
e. Configuring resource controls appropriately
f. Selecting and implementing authentication and encryption technologies

Another example of a system hardening standard is CIS Benchmarks, a collection of more than 100 system hardening configuration guidelines addressing vendor-specific desktops and web browsers, mobile devices, network devices, server operating systems, virtualization platforms, the cloud, and commonly used software applications.

An ideal System Hardening best practice usually contains the following action items:

a. *Have users create strong passwords and change them regularly.*
b. *Remove or disable all superfluous drivers, services, and software.*
c. *Set system updates to install automatically.*
d. *Limit unauthorized or unauthenticated user access to the system.*
e. *Document all errors, warnings, and suspicious activity.*

iv. Although the principles of Asset Hardening are universal across both IT/ICS environments, specific tools and techniques do vary depending on the type of hardening that is carried out and also the hardened ICS assets.

v. Emphasis should be on ICS assets which are in operation, as removing functionality without the proper review and analysis can lead to unexpected issues and system behaviour.

vi. Asset Hardening is needed throughout the lifecycle of ICS assets, from initial installation, through configuration, maintenance, and support, to end-of-life decommissioning. Asset Hardening is also a requirement of regulatory mandates and is increasingly demanded by cyber insurers.

5.2 Initiation of Inspection Process

5.2.1 The concerned function of IB appoints a Team Leader (TL) to initiate the inspection process.

5.2.2 The application is reviewed by the appointed TL for completeness and to obtain confidence that the applicant has clarity of inspection requirements and the capability of IB to provide the required inspection services promptly. IB will review its ability to inspect terms of its policy and process, its competence, and the ability of personnel suitable for inspection activities. The knowledge required for inspecting various controls for IT is defined in Annex B of this section and the capabilities required including baseline skill set in ICS are defined in Annex C of this section. 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. IB 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 an application if there is any adverse finding in the above exercise. The decision of the IB shall be communicated to the applicant CSE with reasons for not accepting the application. The applicant can appeal against such a decision.

5.2.3 Upon deciding to accept the application, the same is recorded or registered and then an inspection team is appointed.

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

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

5.3 Appointment of the Inspection Team

5.3.1 The inspection team, consisting of a TL and the members, is identified by IB from the pool of Inspectors and experts. The inspection team shall include a Technical Expert (if required), in addition to the number of team members having knowledge of inspection criteria and guidance elements for IT and ICS are mentioned in Annex B and Annex C of this section respectively. While finalising the Inspection Team, the role and task performed by each Inspector should be clearly mentioned as various members of the team will have expertise specific to a few controls and not as a whole.

5.3.2 The names of the members of the inspection team for carrying out the document review and the onsite inspection are also communicated along with the CV to the applicant along with the proposal and is requested to inform IB about acceptance of/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 IB will evaluate the objection and decide whether to change the team member or to overrule the objection raised by the applicant. The inspection team is then formally appointed. Efforts are made to ensure that the team is kept intact throughout the initial inspection 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 inspection at the time of their appointment as IB inspector/expert. The team members are required to maintain confidentiality of the sensitive information about the operation of the applicant obtained as part of the inspection process unless required by law, in which case the same will be done under intimation to the applicant.

5.3.3 All IB Inspectors have declared that they have no conflict of interest and are committed to disclosing if such a situation arises so that IB can make appropriate decisions. The police verification/background check of the Inspection Team has been completed for records of the I

5.3.4 If a preliminary visit is requested by the applicant, the IB Secretariat shall organize the same after obtaining the acceptance of the preliminary visit fee by the applicant. Such a visit would solely be to gain a better understanding of the operations of the applicant and for the applicant to better understand the inspection process and clarify the expectations of IB 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 inspection. This has a very limited objective of process acquaintance for both IB and CSEs and is not to be considered as a formal inspection.

5.4 Inspection Requirements

5.4.1 Inspection Criteria

The IB shall use the ‘Inspection Criteria’, as mentioned in Section 4 of this document, as a reference for carrying out the inspection.

5.4.2 Amendment to the Criteria

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

i. Any change in the international standards and guides.
ii. Significant feedback from the Peer Review inspection 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 inspection 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 month and year of the issue.

5.5 Inspection Report

5.5.1 Granting of Inspection Report

a. The CSE is granted and an inspection report after the completion of the inspection and issue of the inspection report to an applicant and after the conditions given below are met by the applicant:

i. The applicant meets the provisions of inspection criteria and all non-conformities and concerns found against the criteria during inspection have been closed to the satisfaction of the IB in accordance with the guidelines on the subject.
ii. There are no adverse reports/information/complaints with the IB about the applicant regarding the quality and effectiveness of the implementation of inspection criteria. There is also no evidence of fraudulent behaviour.

iii. The clients of the CSEs are satisfied by the conduct of the applicant and its infrastructure security provisions. IB may request feedback from selected clients of the applicant / publicize receipt of the application and seek feedback from stakeholders.

iv. The applicant CSE has paid all the outstanding dues.

v. The inspection report shall be valid for a period of 01 year.

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 CSE will be given an opportunity to explain its position in writing to the IB and present its case in person to the certification committee. The final decision shall be taken in respect of granting of statement of compliance on the basis of a review of the facts and the results of such presentation.

c. Once the organisation fulfils all inspection requirements, an inspection report will be issued by IB covering the scope and reference of the inspection criteria and report.

d. IB shall publish on its website, the grant of any new IC, for information and feedback from the industry / other stakeholders.

5.5.2 Continuing compliance with Inspection Criteria

It is recommended that CSEs carry out the inspection w.r.t the inspection criteria with a focus on vulnerability assessment penetration testing at least annually with an independent third-party inspection body and provide a declaration of conformity to this

effect. This is recommended because of:

a. Change in vulnerability landscape (top 10 vulnerabilities are published by professional organisations such as OWAS).

b. The augmentation of IT/ICS infrastructure by CSE.

However, CSE shall strengthen their process for continuous monitoring and patching the vulnerabilities as specified in 5.5.3.

5.5.3 Develop a plan to continuously assess and track vulnerabilities on all CSE assets within their infrastructure, to remediate, and minimize, the window of opportunity for attackers. They shall monitor public and private industry sources for new threat and vulnerability information.

a. Cyber defenders are constantly being challenged by attackers who are looking for vulnerabilities within their infrastructure to exploit and gain access. Defenders must have timely threat information available to them about software updates, patches, security advisories, threat bulletins, etc., and they should regularly review their environment to identify these vulnerabilities before the attackers do. Understanding and managing vulnerabilities is a continuous activity, requiring focus of time, attention, and resources.

b. Attackers have access to the same information and can often take advantage of vulnerabilities more quickly than an enterprise can remediate. While there is a gap in time from a vulnerability being known to when it is patched, defenders can prioritize which vulnerabilities are most impactful to the enterprise, or likely to be exploited first due to ease of use. For example, when researchers or the community report new vulnerabilities, vendors have to develop and deploy patches, indicators of compromise (IOCs), and updates. Defenders need to assess the risk of the new vulnerability to the enterprise, regression-test patches, and install the patch.

c. Attackers might be using an exploit to a vulnerability that is not known within the security community. They might have developed an exploit to this vulnerability referred to as a “zero-day” exploit. Once the vulnerability is known in the community, the process mentioned above starts. Therefore, defenders must keep in mind that an exploit might already exist when the vulnerability is widely socialized. Sometimes vulnerabilities might be known within a closed community (e.g., vendor still developing a fix) for weeks, months, or years before it is disclosed publicly. Defenders have to be aware that there might always be vulnerabilities they cannot remediate, and therefore need to use other controls to mitigate.

d. CSEs that do not assess their infrastructure for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their assets compromised. Defenders face particular challenges in scaling remediation across a CSE, and prioritizing actions with conflicting priorities, while not impacting the business or mission. CSEs shall consider to:

i. Establish and Maintain a Vulnerability Management Process
ii. Establish and Maintain a Remediation Process
iii. Perform Automated Operating System Patch Management
iv. Perform Automated Application Patch Management
v. Perform Automated Vulnerability Scans of Internal Enterprise Assets
vi. Perform Automated Vulnerability Scans of Externally Exposed Enterprise Assets
vii. Remediate Detected Vulnerabilities

5.6 Inspection

The inspection shall be for the capability of the CSEs to operate a sound framework in compliance with the inspection criteria and inspection process.

5.6.1 Preparation for the Inspection Plan

a. The IB prepares an inspection plan for the conduct of the initial inspection process covering two stages as follows:

i. Stage 1 - Detailed review of the applicant's IT/ICS infrastructure-related documentation: This shall cover all applicable levels of documents of the CSEs covering procedures for controls defined in IC.

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

The normal inspection duration for each stage is described in Annex A of this section. The draft inspection plan may be prepared in stages as mentioned above depending on the information supplied and when the inspection activity is planned.

iii. All locations (such as branch/sub-contractor's offices, if is under the scope of CII) mentioned in the scope of inspection shall be covered. Inspection plan

The lead inspector shall prepare an inspection plan after studying the depleted system architectures, reviewing of asset database, identifying tools for inspection planning, conducting VAPT and planning for configuration review by use of a security configuration checklist.

Note: A security configuration checklist (also called a lockdown, hardening guide, or benchmark) is a series *of instructions or procedures for configuring an IT product to a particular operational environment, for verifying that the product has been configured properly, and/or for identifying unauthorized changes to the product. The IT product may be commercial, open source, government-off-the-shelf (GOTS), etc. Checklists can comprise templates or automated scripts, patch information, Extensible Markup Language (XML) files, and other procedures. Checklists are intended to be tailored by each organization to meet its particular security and operational requirements. Typically, checklists are created by IT vendors for their products; however, checklists are also created by other organizations, such as academia, consortia, and government agencies. The use of well-written, standardized checklists can markedly reduce the vulnerability exposure of IT products. Checklists can be particularly helpful to small organizations and to individuals with limited resources for securing their systems.*

The Lead inspector shall identify benchmarks in consultation with the SPOC of the CSEs in this pass-of inspection plan, consideration to the following shall be given.

a. Inputs from NIST vulnerability data base. (NVD)

The NVD is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, product

names, and impact metrics.

b. Inputs from CIS Benchmarks

CIS provides a set of benchmarks (examples given below) Lead inspector after discussion with SPOC CSE shall identify the applicable benchmarks based on CSEs' policies and deploy architecture.

Cloud Providers	Desktop Software	DevSecOps Tools	Mobile Devices	Multi-Function Print Devices
Alibaba Cloud	Microsoft Exchange Server	Software Supply Chain Security	Apple iOS	Print Devices
Amazon Web Services	Microsoft Office		Google Android	
Google Cloud Computing Platform	Zoom			
Google Workspace	Google Chrome			
IBM Cloud Foundations	Microsoft Web Browser			
Microsoft 365	Mozilla Firefox			

c. Proprietary benchmarks applied by OEM or technology suppliers (e.g. Microsoft etc.)

d. CSEs own policies

5.6.2 Inspection Report

a. The inspection team shall prepare a report at each stage The report at each stage of inspection shall be sent by the IB inspection team within prescribed timelines. If no comments are received within a week, then the report is 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 IB, the IB will reserve the right to reject the application. The fees paid by such applicants will be forfeited. In such an event, the decision of the IB 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 IB, with respect to guidelines on the subject and shall be presented to the relevant committee for its decision on the grant of IC to the applicant CSE.

Since PT and VA are core critical processes of Inspection, implementation guidelines

on Penetration Testing are provided in Annex E of this section which are informative in nature. Similarly, a sample Test Report Format (TRF) is provided in Annexure F and Annexure G for PT and VA of this section respectively.

d. Reinspection
Once CSE confirms that they have taken corrective/preventive options, reinspection including the next round of re-inspection including VAPT gives confidence that the system is hardened leading to improvement in security posture.

5.7 Decision for issuing Inspection Report

5.7.1 The reports are presented to the relevant committee of IB along with recommendations for the decision of inspection status.

5.7.2 If the relevant committee of IB is satisfied with the presentation of findings leading to compliance with the inspection criteria, as recommended by the lead inspector, the inspection report is granted to the CSE.

5.8 Complaints and Appeals

5.8.1 Complaints

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

i. the IB, its operation and/ or process
ii. the Inspectors, experts, committee members or staff of the IB
iii. audit process followed by the Inspectors and/or by the IB
iv. misuse of the inspected status either in scope or in use of the inspection body mark or symbol
v. clients of CSEs

b. The complaint shall be made in writing (by any means such as letter/ email etc.) to the IB with complete details of the complainant (name, address, organization etc.) and a 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 IB. If so, the IB validates the complaint based on verification of all necessary information gathered and then the complaint is registered and the IB process for handling complaints is followed.

d. The IB 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 IB, the complainant shall be informed of the same while providing possible assistance like referring the complaint to the concerned by inspection body.

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

f. In case the complaint pertains to other inspections but relates to IB-inspected CSEs, then the concerned IB is informed, and efforts are also made to seek information from the inspected CSEs. Based on any inputs received from the inspected CSEs, the

complainant is advised to follow up with the IB. IB also pursues with the other IB.

g. If the complaint is against the non-compliance of inspection criteria by any applicant or inspected CSEs, then IB shall encourage the complainant to utilize the complaint handling process of the relevant CSEs. At the same time, IB shall also gather all necessary information for establishing the validity of the complaint. If the complainant insists and the CSEs agree, then IB may carry out the investigation. The report of the analysis or parts thereof 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 an inspected CSE, the complaint would be referred to the inspected CSE for possible resolution. If the complainant is not satisfied with the response of the inspected CSEs, the complaint will be taken up further.

i. In case the complaint is received through some other organization/stakeholder, and not directly from the complainant, then the organization would be briefed on the outcome at the end of the process.The decision to be communicated to the complainant will be made /reviewed and approved by individuals not involved in the activities in question.

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

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

l. IB will give a formal notice at the end of the complaint handling process to the complainant.

m. IB will ensure that investigation and decision on complaints do not result in any discriminatory actions.

5.8.2 **Appeals**

a. Any IB applicant/certified CSEs can file an appeal against the decision of the IB 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 IB along with all the necessary information/documents in support of the appeal.

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

5.8.3 **Records**

IB 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.

5.8.4 **Publishing of the Information for Public & availability of Inspection Scheme**

a. The IB shall make public announcements of the inspection Scheme, criteria of inspection, application for inspection, fee schedule and other related documents on its website and specific requests.

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

c. The inspection Schemes are open to all applicants within the capability and scope of the IB.

d. The IB shall also make public information about the suspension withdrawal of inspection status, withholding of recertification and extension of validity of inspection status.

6. Confidentiality and Disclosure

The information obtained regarding the IT/ICS infrastructure of the applicant and inspected CSEs that are not of the nature of public information, shall be kept confidential by all the personnel, members of the IB, panel of Inspectors, experts and the committee members. If the IB 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.

7. Use of Scheme Mark

7.1 The Scheme mark is associated with the organisations that have been inspected by IB as per the applicable requirements and criteria.

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

7.3 The inspection body at the time of the inspection, will inform the client about the use of Scheme mark/mark for display and publicity.

7.4 The inspected client shall submit to the inspection body the form in which he proposes to use the certificate of registration and Scheme mark.

7.5 The inspected client shall not use the Scheme mark/mark, which misleads the information.

7.6 Upon suspension or withdrawal/cancellation of inspection status/ marks in all the products/publicity material to be withdrawn immediately.

8. Termination

8.1 If inspection status is withdrawn from the inspected organization in full, the organization shall immediately cease the use and distribution of any certificates, stationery and literature bearing the Scheme mark.

8.2 If inspection status is withdrawn from an inspected organization in respect of some of its activities, the organization shall immediately cease the use and distribution of any stationery and literature bearing the Scheme mark.

8.2.1 Use of mark (Accreditation body's mark) – As specified by the Accreditation body.

8.2.2 All inspected CSEs are permitted to use Scheme Mark as per the 'Section 7: Rules for Use of Scheme Mark'.

Annexure A

Duration for Inspection

The following components are required to define the inspection duration which shall be as follows for the minimum requirements.

i. Inspection stage 1 – Document review (Manuals, process, other documents as needed – minimum 3 man-days for initial inspection

ii. Review of corrective actions and revised documents – to be estimated based on actual efforts (not less than one man-day) by the IB Secretariat.

iii. Inspection stage 2 – Onsite – Minimum 4 man-days, lead inspector to estimate based on the complexity of infrastructure and architecture, and for calculation of man-days refer to the note below. The need for any additional man-days for specific situations would be estimated by the IB Secretariat and informed to the CSEs in advance.

iv. Branch office / sub-contractor if covered under the scope of CII – minimum 1 man-day depending on the activities carried out in the branch.

v. Follow-up inspections– To be estimated by IB.

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

vii. Review of response to NCs – as per actuals (may be done virtually)

viii. Penetration Testing – minimum 4 days (covering 100% IPs open to the public)

ix. Vulnerability Assessment – as per actuals, a minimum of 0.5 man-days per device scanning

ix. Overall time – based on the architecture and components (software, hardware, firmware, OS etc.) The IB shall define a procedure for this. The following may be considered:

- 30% of total devices/components/sub-systems. The samples should represent the whole population of inspection objects (software, hardware, firmware, OS etc.) based on functional, structural, and logical similarity ensuring selection is statistically significant.

- 100% for critical systems, and sub-systems depending on their functional position in the architecture.

Annexure B

Knowledge Areas for Inspection Team for each control (IT)

S No.	Control	Description
1.	Inventory and Control of Enterprise Assets	Knowledge of actively managing inventory and tracking all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise.
2.	Inventory and Control of Software Assets	Knowledge of actively managing inventory and tracking all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.
3.	Data Protection	Knowledge of developing processes and technical controls to identify, classify, securely handle, retain, and dispose of data.
4.	Secure Configuration of Enterprise Assets and Software	Knowledge of establishing and maintaining the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).
5.	Account Management	Knowledge of using processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.
6.	Access Control Management	Knowledge of using processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.
7.	Continuous Vulnerability Management	Knowledge of developing a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.
8.	Audit Log Management	Knowledge of collecting, reviewing and retaining audit logs of events that could help detect, understand, or recover from an attack.
9	Email and Web Browser Protections	Knowledge of improving protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behaviour through direct engagement.

10.	Malware Defenses	Knowledge of preventing or controlling the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.
11.	Data Recovery	Knowledge of establishing and maintaining data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state. Knowledge of simulation of test environment.
12.	Network Infrastructure Management	Knowledge of establishing, implementing and actively managing (tracking, reporting, correcting) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.
13.	Network Monitoring and Defense	Knowledge of operating processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.
14.	Security Awareness and Skills Training	Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.
15.	Service Provider Management	Knowledge of developing a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.
16.	Application Software Security	Knowledge of managing the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise. Knowledge of OWASP top 10 vulnerabilities.
17.	Incident Response Management	Knowledge of establishing a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.
18.	Penetration Testing	Knowledge and skill in testing the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker. Knowledge of test planning and management, test case design and use of penetration test tools. ICS security measures should not have the potential to cause the loss of essential services and functions, including emergency procedures. (IT security measures, as often deployed, do have this potential.) ICS security goals focus on control system availability, plant protection, plant operations (even in a degraded mode) and time-critical system response. IT security goals often do not place the same emphasis on these factors; they may be more concerned with protecting information rather than physical assets. These different goals need to be clearly stated as security objectives regardless of the degree of plant integration achieved.

Annexure C

Knowledge Areas for Inspection Team for each control (ICS)

S No.	Control	Description
1.	Inventory and Control of Hardware Assets	• Knowledge of lifecycle and acquisition costs • Knowledge on approval process and the technical drawings and automated inventory systems • Knowledge of inventory and device visibility in an ICS environment where network segmentation, dual homing and isolation are a common theme. • Knowledge of management of new and old devices from multiple vendors some of which are not IP-based. • Knowledge of the process of inspection of devices in a hostile environment.
2.	Inventory and Control of Software Assets	• Knowledge of ICS manufacturers and vendors providing a list of recommended and supported software and versions that are required for each system. • Knowledge of forecasting operating systems and application lifecycle cost in alignment with typical COTS (commercial off-the-shelf software) End of Life and End of Support (EoL/EoS) Notifications. • Knowledge of ensuring cybersecurity requirements is a consideration within procurement/sourcing processes. Specifically, vendors leverage a secure development lifecycle.
3.	Continuous Vulnerability Management	• Knowledge of the process and tools for performing active vulnerability scanning, caution required to avoid adversely affecting ICS network communications and in turn, product, and system availability. • Knowledge of network stack sensitivity, limited resources, or other situational factors. Conduct scanning during process outages such as regularly scheduled maintenance or planned shutdowns. • Knowledge of operating system and application updates, security patches, and service packs. • Knowledge on creating a test bed that mimics a production environment for specific patch regression testing prior to implementing in production ICS environments.
4.	Control use of administrative privileges	• Knowledge of minimizing the use of elevated privileges and only using administrative accounts where they are required specific to the ICS environment.
5.	Secure Configurations for hardware and software on devices, laptops, workstations and servers	• Knowledge of configuration management tools is used. • Knowledge on process on set to alert-only without automated configuration re-deployment unless considered safe.
6.	Maintenance, monitoring	• Knowledge on leveraging an IT-based SIEM which

	and analysis of audit norms	supports the ICS environment because many logging analytic and alerting solutions do not support or correctly interpret or correlate ICS-specific events.
7.	E-mail and web browser protection	• Knowledge of ensuring that all systems are segmented such that there is no Internet web access. • Knowledge of ensuring that no email clients are installed or present on any systems.
8.	Malware Defenses	• Knowledge of ensuring Anti-malware tools needs to be properly regression-tested to ensure that the availability and reliability of the system will not be adversely affected. • Knowledge that this testing should take place whenever a change is made to the anti-malware software such as a configuration change, software hotfix, or repository update. • Knowledge of ensuring anti-malware tools are configured such that a false positive detection will not negatively impact the availability or reliability of any critical processes.
9.	Limitation and control of network ports, protocols and services	• Knowledge of inventorying open or available network ports, and the process or tools used should be non-intrusive and not impact the availability or reliability of the system. • The knowledge that in the ICS environment, most systems are considered critical and mail servers should not be present in ICS networks.
10.	Data Recovery Capabilities	• Knowledge that system backups and recovery procedures are documented.
11.	Secure Configurations for network devices such as firewalls, routers and switches	• Knowledge of tools and procedures to ensure that the firewalls are configured to deny by default.
12.	Boundary Defence	• Knowledge of reviewing deployed architecture to ensure ICS networks are not directly connected to the internet.
13.	Data Protection	• Knowledge of ensuring sub-controls related to automated and scheduled scanning might adversely affect the reliability of the system. Only scanning for sensitive data when it is safe to do so.
14.	Controlled access based on need to know	• Knowledge on ensuring that authorized individuals and/or systems are restricted in how they communicate with other systems necessary to fulfil their specific responsibilities. • Knowledge of ensuring safeguarding communications and operating as a mechanism of access control and isolating communications.
15.	Wireless access control	• Knowledge of ensuring software security patches and product upgrades are applied throughout the wireless infrastructure and products are kept current throughout

		their lifecycle. • Knowledge on ensuring that wired devices do have aspects of physical security that wireless devices may not similarly enjoy.
16.	Account monitoring and control	• Knowledge of ensuring a mechanism for changing shared account passwords immediately upon termination of any workforce member knowing the credentials. • Knowledge of restricting shared operator account permissions to limit system access and changes.
17.	Implement security awareness and training programme	• Knowledge of implementing a security awareness program that is mandated for completion by all visitors (Including 3rd parties: contractors, subcontractors, vendors, etc.) prior to granting remote or on-premises site access. • Knowledge of training people for risk of non-compliance on the concerned processes.
18.	Application Software Security	• Knowledge of ensuring that the most current and relevant patch or software version is used, avoiding older versions that may contain known or unknown vulnerabilities also adds to helping with software assurance. • Knowledge of top 10 vulnerabilities for ICS environment, tools, and procedures for application security testing.
19.	Incident response and management	• Knowledge of ensuring that the Incident Response Plan has been reviewed and approved by ICS Operational Leadership. • Knowledge of the conduct of cyber drills in the ICS environment. • Knowledge of instrumentation and tools for IR and management.
20.	Penetration Tests and Red Team Exercise	• Knowledge of tools, instrumentation, and test environment on Penetration Testing. • Knowledge of the procedure of Pen Test (test management, test case design, testing scenario and analysis of test results) in an ICS environment. • Knowledge on special considerations in ICS environment considering specific availability requirements of ICS.

Annexure D

Capabilities and baseline skill set requirements for techniques used in Inspection for IT and ICS
(Informative)

1. **Review Techniques**

Technique	Capabilities	Baseline Skill Set
Documentation Review	• Evaluates policies and procedures for technical accuracy and completeness	• General knowledge of security from a policy perspective
Log Review	• Provides historical information on system use, configuration, and modification • Could reveal potential problems and policy deviations	• Knowledge of log formats and ability to interpret and analyze log data; ability to use automated log analysis and log correlation tools
Ruleset Review	• Reveals holes in ruleset- based security controls	• Knowledge of ruleset formats and structures; ability to correlate and analyze rule sets from a variety of devices
System Configuration Review	• Evaluates the strength of system configuration • Validates that systems are configured in accordance with hardening policy	• Knowledge of secure system configuration, including OS hardening and security policy configuration for a variety of operating systems; ability to use automated security configuration testing tools
Network Sniffing	• Monitors network traffic on the local segment to capture information such as active systems, operating systems, communication protocols, services, and applications • Verifies encryption of communications	• General Transmission Control Protocol/Internet Protocol (TCP/IP) and networking knowledge; ability to interpret and analyze network traffic; ability to deploy and use network sniffing tools
File Integrity Checking	• Identifies changes to important files; can also identify certain forms of unwanted files, such as well-known attacker tools	• General file system knowledge; ability to use automated file integrity checking tools and interpret the results

2. Target Identification and Analysis Techniques

Technique	Capabilities	Baseline Skill Set
Network Discovery	• Discovers active devices. • Identifies communication paths and facilitates determination of network architectures	• General TCP/IP and networking knowledge; ability to use both passive and active network discovery tools
Network Port and Service Identification	• Discovers active devices. • Discovers open ports and associated services/ applications	• General TCP/IP and networking knowledge; knowledge of ports and protocols for a variety of operating systems; ability to use port scanning tools; ability to interpret results from • tools
Vulnerability Scanning	• Identifies hosts and open ports • Identifies known vulnerabilities (note: has high false positive rates) • Often provides advice on mitigating discovered vulnerabilities	• General TCP/IP and networking knowledge; knowledge of ports, protocols, services, and vulnerabilities for a variety of operating systems; ability to use automated vulnerability scanning tools and interpret/analyze the results
Wireless Scanning	• Identifies unauthorized wireless devices within range of the scanners • Discovers wireless signals outside of an organization's perimeter • Detects potential backdoors and other security violations	• General knowledge of computing and radio transmissions in addition to specific knowledge of wireless protocols, services, and architectures; ability to use automated wireless scanning and sniffing tools

3. Target Vulnerability Validation Techniques

Technique	Capabilities	Baseline Skill Set
Password Cracking	• Identifies weak passwords and password policies	• Knowledge of secure password composition and password storage for operating systems; ability to use automated cracking tools
Penetration Testing	• Tests security using the same methodologies and tools that attackers employ. • Verifies vulnerabilities. • Demonstrates how vulnerabilities can be exploited iteratively to gain greater access	• Extensive TCP/IP, networking, and OS knowledge; advanced knowledge of network and system vulnerabilities and exploits; knowledge of techniques to evade security detection
Social Engineering	• Allows testing of both procedures and the human element (user awareness)	• Ability to influence and persuade people; ability to remain composed under pressure

Annexure E

Implementation Guidelines on Penetration Testing

1. The objectives of conducting a pen test are

    a. To gauge how rigorous CSE's defenses are and how well the system tolerates a real-world attack.
    b. To discover the necessary level of sophistication an attacker would need to have successfully compromised the cybersecurity defenses.
    c. To determine further countermeasures that could limit threats to the system.
    d. To learn how effectively a CSE can detect an attack and then respond to it.

2. Common vulnerabilities include

    a. Misconfigurations: Misconfigured security settings or partially insecure default settings.
    b. Kernel flaws| The Kernel code which is the central aspect of an OS: is in charge of executing the total security model.
    c. Buffer overflows: If programs don't properly address input for the right length, arbitrary code with administrator-level privileges may enter the system.
    d. Insufficient input validation: When applications fail to validate the input they receive from users, it exposes the system to SQL injection attacks.
    e. Symbolic links: Also known as a symlink, this type of file sends you to another file. Symlinks could be exploited to compromise system files.
    f. Race conditions: If a program is in privileged mode, a user can carefully time their attack, using the elevated privileges as an entryway.
    g. Incorrect file and directory permissions: Improper permissions could possibly expose your system to a host of different attacks.

3. Penetration test scenarios should focus on locating and targeting exploitable defects in the design and implementation of an application, system, or network. Tests should reproduce both the most likely and most damaging attack patterns including worst-case scenarios such as malicious actions by administrators.

4. Penetration testing empowers an organisation to

    a. Identify security gaps and exposures.
    b. Prioritize cybersecurity risks.
    c. Discover misconfigurations and backdoor exploits.
    d. Understand all potential attack vectors.
    e. Respond to a breach quickly and effectively.

5. There are two forms of pen testing

    a. **External Pen Test (EPT):**
    External pen testing takes place from outside CSE's security perimeter. Also known as black hat testing, it allows CSE to measure security posture as it would appear to outsiders that sought entry into the network (typically via the internet); the tester starts with zero knowledge of the CSE cybersecurity environment. The goal of the external pen test is to reveal vulnerabilities that could be exploited by a malicious attacker. The following terms are associated with EPT:

        i. **Reconnaissance:** Tester goes on a fact-finding mission, scouring the internet for publicly available information such as:

- DNS server information
- IP addresses
- OS
- Newsgroup postings

ii. **Enumeration** – Tester uses discoveries and scanning techniques to find external hosts as well as listening services.

iii. **Evasion** – Tester applies evasion techniques to circumvent common perimeter defenses like:

- Firewalls
- Routers
- Access controls

iv. **Initial attacks** – Tester sends the opening salvo of attacks in order to test the response of common application protocols.

v. **Vulnerability attacks** – After finding servers that are externally accessible, the tester seeks to gain access to internal servers and sensitive information.

vi. **Continued discovery** – Tester looks for alternative access method exposures, including:

- Wireless access points
- Modems
- Portals to internal servers

b. Internal Pen Test

Internal testing gives the attacker a head start of sorts. They're provided information beforehand, which allows them to simulate an attack from an employee. This means they start from a privileged position. An internal pen test reveals exploitable vulnerabilities, particularly those related to system-level security and configurations, including:

i. Authentication
ii. Access control
iii. System hardening
iv. Application configuration
v. Service configuration
vi. Usually, the tester begins with at least some level of access to the network, with the same privileges and information a typical user would have; although

they could be granted even more privileges, depending on your specific goals of the test.

The tester's goal is to gain further access to other networks and systems via privilege escalation. From there, the mission is to determine how deep into a network a hacker could go as well as how much damage could potentially be done.

6. The Pentest Framework Phases

Whether the pen test is internal or external, penetration testing framework focuses on four overarching phases:

a. **Planning:** The planning phase represents the pre-phase of penetration testing. During this initial stage, the pen tester will meet with your organization to outline the specifics of the test, including:

- Expectations
- Objectives
- Goals
- Legal implications

Note: The tester seeks to gain a deep understanding of risks, culture, and what types of tests need to be done. After rules have been identified, management approval with documentation is obtained.

b. **Discovery:** The tester begins the initial process of testing, which is intended to gather information and scan systems. Depending on the attacker, there are several different techniques that can be used to gather crucial details, including:

- Network port and service identification – Tester uses a port scanner to identify:
- Network ports
- Services currently operating on active hosts.
- Applications running on each identified service.

The next part of the discovery phase involves vulnerability analysis.

During this stage, the tester will gather the services, applications, and OS of scanned hosts. They will then compare those categories against vulnerability databases and the tester's own knowledge.

This can be done using either digital or manual processes. Manual processes take longer but may be able to identify vulnerabilities that an automatic scanner could miss.

c. **Attack:** "Executing an attack is at the heart of any penetration test." Typically, the attack phase follows four steps, which are then repeated if successful:

- Gaining access – If an attack is successful, the vulnerability is confirmed, and possible mitigating responses are listed. Most exploits don't allow the tester

to have the max level of access; rather they tend to teach the tester more about the network and its vulnerabilities.

- Escalating privileges – In some cases, an exploit may allow the tester to escalate their privileges on the network or system to ascertain the true risk level.
- System browsing – Information gathering processes allow testers to identify new ways to gain access to additional systems.
- Install additional tools – If the tester gets this far they can install more tools on the system or network, which would then enable them to delve into additional systems or resources.

d. Reporting

Once the test is finished, the testing team will prepare a comprehensive report that includes:

- Known vulnerabilities
- Present risk ratings
- Remediation guidance
- Repeat the test at least annually.

7. Penetration Testing in ICS Environment

It shall be done with care to ensure that ICS functions are not adversely impacted by the testing process. These systems are highly sensitive to timing constraints and have limited resources. E.g.: compensating controls include employing a replicated, virtualised or simulated system to conduct pen tests. Production ICS may need to be taken off-line report testing can be conducted, test shall be scheduled to occur during planned ICS outages whenever possible. If a pen test is performed on non-ICS methods, extra care is taken to ensure that the test doesn't propagate into the ICS network for which specific expertise is necessary. It may not be feasible to identify personnel with appropriate skill sets to perform this test in this situation, especially for high-impact ICS systems.

Annexure F

Test Report Format (TRF) for Penetration Testing

SRF & PROPOSAL No.	Penetration Test Report ID	Date	Page

1.0	**Client / CSE Details**	
1.1	Client / CSE	
1.2	Address of the Client / CSE	
2.0	**Details of the Software System Under Test**	
2.1	Project	
2.2	Software Version No.	
2.3	Software Release Date	
2.4	System Description	
2.5	Software Application Developing Organization	
2.6	Applicable Reference Documents	
2.7	Software Application Supplied Media/ Access	
2.8	Software Application Documents Submitted	
3.0	**Test Description**	
3.1	Name & Address of the Testing Organization	
3.2	Test Objective(s)	
3.3	Scope of Testing	
3.4	Type of Testing	
3.5	Test Approach & Methodology	
3.6	Test Standards	
3.8	Test Environment	
	Hardware Configurations	
	Software Configurations	
3.9	Test Location	
3.10	Test Team	
3.11	Period of Testing	

4.0 Observations

S. No.	Parameter	Observation	Status
1.	Network Survey		
1.1	Discovery from Public Resources		
1.2	Ping & Trace Route		
1.3	Discovery from site		
2.	Port Scanning		
2.1	Open and Closed Port		
3.	Finger Printing		
3.1	OS fingerprinting		
4.	Service Probing		
4.1	SSL used		
5.	Vulnerability Analysis		
5.1	Missing Secure Attribute in Encrypted Session (SSL) Cookie		
5.2	SHA-1 cipher suites were detected		
5.3	Cacheable SSL Page Found		
5.4	Missing "X-Content-Type- Options" header		
5.5	Missing "X-XSS-Protection" header		
5.6	Missing HTTP Strict- Transport-Security Header		
5.7	Invalid date in “Expires” header		
6.	Exploit attempted		
6.1	Zone Transfer		

Observations:

5.0 Approval:

Approved by: **Released by:**

Head QA Head (CSC)

Annexure G

Test Report Format (TRF) for Vulnerability Assessment

SRF & PROPOSAL No.	Vulnerability Assessment Report ID	Date	Page

1.0	**Client/CSE Details**	
1.1	Client/ CSE	
1.2	Address	
2.0	**Details of the Projects**	
2.1	Project	
2.2	Applicable Reference Documents	
2.3	Project Developer	
2.4	Documents Submitted	
3.0	Testing Description	
3.1	Testing Organization	
3.2	Testing Objectives	
3.3	Scope of Testing	
3.4	Type of Testing	
3.5	Location of Testing	
3.6	Reference Standards	
3.7	Testing Cycle	
3.8	Testing Methodologies	
3.9	Network Diagram	
3.10	Testing Team	
3.11	Duration of Testing	

4. Key summary

Severity Classification

Severity	Description

Critical	An aspect of a critical requirement which is deficient or vulnerable to direct or indirect attack that will create decisive or significant effects.
High	The threat-source is highly motivated and sufficiently capable. This makes it possible for a remote attacker to violate the security protection of a system (i.e., gain some sort of user, root or application account), or permits a local attack that gains complete control of a system. Exercise of the vulnerability may result in the highly costly loss of major tangible assets or resources; may significantly violate, harm, or impede an organization's mission, reputation, or interest.
Medium	The threat-source is motivated and capable. Remote attackers may violate/ exploit the application. Exercise of the vulnerability may result in the costly loss of tangible assets or resources; may violate, harm, or impede an organization's mission, reputation, or interest.
Low	The threat-source lacks motivation or capability. The vulnerability typically does not yield valuable information or control over a system but rather gives the attacker knowledge to provide the attacker with information that may help him find and exploit other vulnerabilities. Exercise of the vulnerability may result in the loss of some tangible assets or resources or may noticeably affect an organization's mission, reputation, or interest.
Pass	The hardening of host is as per CIS benchmark.
Fail	The hardening of host is not properly configured which may lead to compromise the host.
Warning	The hardening of the host is not properly configured. However, it is not a potential threat.
Compliance	The configuration is set as per the security requirement.
Not in Compliance	The configuration is not set as per the security requirement.

4.0 Vulnerability Assessment Summary

4.1 CIS Benchmark Compliance/Hardening Summary of OS

1st Cycle

S No.	Host Name	IP Address	OS Type	Application /Role	Status		
					Pass	Warning	Fail

Final Cycle

S No.	Host Name	IP Address	OS Type	Application /Role	Status			
					Pass	Warning	Fail	Justification Accepted

*** Closed based on Justification and Implementation plan.**

4.2 Plug-in Vulnerabilities summary of OS: 1st Cycle

S No.	Host Name	IP Address	OS Type	Application /Role	Severity			
					Critical	High	Medium	Low

Final Cycle

S No.	Host Name	IP Address	OS Type	Application /Role	Severity				
					Critical	High	Medium	Low	Justification Accepted

4.3 Compliance Summary of <Cloud Platform>, <container design platform>, automation server, Internal Firewall 1st Cycle

S No.	Devices	In Compliance	Not in Compliance
1.			

Final Cycle

S. No.	Devices	In Compliance	Not in Compliance

5.0 Test Findings

5.1 Findings of OS level

Compliance

S. No	Compliance Point	Compliance Status	Final Remark
01.	Findings of OS level		
02.	Ensure sticky bit is set on all world-writable directories		
03.	Ensure boot loader password is set		
04.	Ensure authentication required for single user mode		
05.	Ensure ALSR is enabled		
06.	Ensure App Armor profiles are enforcing Complain mode		
07.	Ensure message of the day is configured properly		
08.	Ensure Local login warning banner is configured properly		
09.	Ensure Remote login warning banner is configured properly		
10.	Ensure updates. Patches and additional security software are installed		
11.	Ensure NFS and RPC are not enabled		
12.	Ensure telnet client is not installed		
13.	IP forwarding and IP redirect		
14.	Ensure /etc/host.allow is configured		
15.	Ensure /etc/host.deny is configured		
16.	Ensure default deny firewall policy-Chain forward		
17.	Ensure Loopback traffic is configured		
18.	Ensure events that modify the system's network environment are collected - /etc/sysconfig/network		
19.	Ensure use of privileged commands is collected		
20.	Ensure kernel module loading and unloading is collected - auditctl init_module/delete_module (32-bit)		
21.	Ensure SSH Permit User Environment is disabled		
22.	Ensure SSH access is limited		
23.	Local Password for users		
24.	Ensure system accounts are non-login		

25.	Ensure default user shell timeout is 900 seconds or less - /etc/bashrc		
26.	Ensure no world writable files exist		
27.	Ensure no unowned files or directories exist		
28.	Ensure users' home directories permissions are 750 or more restrictive		
29.	Ensure users' dot files are not group or world writable		

Vulnerabilities

S. No	Host Name	IP Address	Vulnerabilities	Severity	Justification	Final Remark

5.2 Findings of <Cloud Platform>

S No.	Description	Observation	Status	Clients Action	Final Remarks
1	**Identity and Access Management**				
1.1	Maintain current contact details (Manual)				
1.2	Ensure security contact Information is registered (Manual)				
1.3	Ensure security questions are registered in the <Cloud Platform> account (Manual)				
1.4	Ensure no root user account access key exists (Automated)				
1.5	Ensure MFA is enabled for the "root user" account (Automated)				
1.6	Ensure hardware MFA is enabled for the "root user" account (Automated)				
1.7	Eliminate use of the root user for administrative and daily tasks (Automated)				
1.8	Ensure IAM password policy requires minimum length of 14 or greater (Automated)				
1.9	Ensure IAM password policy prevents password reuse (Automated)				

1.10	Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password (Automated)				
1.11	Do not setup access keys during initial user setup for all IAM users that have a console password (Manual)				
1.12	Ensure credentials unused for 90 days or greater are disabled (Automated)				
1.13	Ensure there is only one active access key available for any single IAM user (Automated)				
1.14	Ensure access keys are rotated every 90 days or less (Automated)				
1.15	Ensure IAM Users Receive Permissions Only Through Groups (Automated)				
1.16	Ensure IAM policies that allow full "*:*" administrative privileges are not attached (Automated)				
1.17	Ensure a support role has been created to manage incidents with <Cloud Platform> Support (Automated)				

1.18	Ensure IAM instance roles are used for <Cloud Platform> resource access from instances (Manual)				
1.19	Ensure that all the expired SSL/TLS certificates stored in <Cloud Platform> IAM are removed (Automated)				
1.20	Ensure that S3 Buckets are configured with 'Block public access (bucket settings)' (Automated)				
1.21	Ensure that IAM Access analyzer is enabled (Automated)				
1.22	Ensure IAM users are managed centrally via identity federation or <Cloud Platform> Organizations for multi- account environments (Manual)				
2	**Storage**				
2.1	Simple Storage Service (S3)				
2.1.1	Ensure all S3 buckets employ encryption-at-rest (Manual)				
2.1.2	Ensure S3 Bucket Policy allows HTTPS requests (Manual)				
2.2	Elastic Compute Cloud (EC2)				
2.2.1	Ensure EBS volume encryption is enabled (Manual)				
3	**Logging**				
3.1	Ensure CloudTrail is enabled in all regions (Automated)				

3.2	Ensure CloudTrail log file validation is enabled (Automated)				
3.3	Ensure the S3 bucket used to store CloudTrail logs is not publicly accessible (Automated)				
3.4	Ensure CloudTrail trails are integrated with Cloud Watch Logs(Automated)				
3.5	Ensure <Cloud Platform> Config is enabled in all regions (Automated)				
3.6	Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket (Automated)				
3.7	Ensure CloudTrail logs are encrypted at rest using KMS CMKs (Automated)				
3.8	Ensure rotation for customer created CMKs is enabled (Automated)				
3.9	Ensure VPC flow logging is enabled in all VPCs (Automated)				
3.10	Ensure that Object-level logging for write events is enabled for S3 bucket (Automated)				
3.11	Ensure that Object- level logging for read events is enabled for S3 bucket (Automated)				
4	**Monitoring**				

4.1	Ensure a log metric filter and alarm exist for unauthorized API calls (Automated)				
4.2	Ensure a log metric filter and alarm exist for Management Console sign-in without MFA (Automated)				
4.3	Ensure a log metric filter and alarm exist for usage of "root" account (Automated)				
4.4	Ensure a log metric filter and alarm exist for IAM policy changes. (Automated)				
4.5	Ensure a log metric filter and alarm exist for CloudTrail configuration changes (Automated)				
4.6	Ensure a log metric filter and alarm exist for <Cloud Platform> Management Console Authentication failures (Automated)				
4.7	Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer created CMKs. (Automated)				
4.8	Ensure a log metric filter and alarm exist for S3 bucket Policy changes. (Automated)				
4.9	Ensure a log metric filter and alarm exist for <Cloud Platform> Config configuration changes (Automated)				

4.10	Ensure a log metric filter and alarm exist for security group changes. (Automated)				
4.11	Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL) (Automated)				
4.12	Ensure a log metric filter and alarm exist for changes to network gateways (Automated)				
4.13	Ensure a log metric filter and alarm exist for route table changes (Automated)				
4.14	Ensure a log metric filter and alarm exist for VPC changes (Automated)				
5.	Networking				
5.1	Ensure no Network ACLs allow ingress from 0.0.0.0/0 to remote server administration ports. (Automated)				
5.2	Ensure no security groups allow ingress from 0.0.0.0/0 to remote server administration port. (Automated)				
5.3	Ensure the default security group of every VPC restricts all traffic (Automated)				

5.4	Ensure a log metric filter and alarm exist for <Cloud Platform> Config configuration changes (Automated)				
5.5	Ensure a log metric filter and alarm exist for security group changes. (Automated)				
5.6	Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL) (Automated)				
5.7	Ensure a log metric filter and alarm exist for changes to network gateways (Automated)				
5.8	Ensure a log metric filter and alarm exist for route table changes (Automated)				
5.9	Ensure a log metric filter and alarm exist for VPC changes (Automated)				
5.10	Ensure a log metric filter and alarm exists for <Cloud Platform> Organizations changes (Automated)				

5.3 Findings of <Automation Server>

S. No.	Assessment Points	Observations	Status	Client's Action	Final Remark
1	**Authentication**				

S. No.	Assessment Points	Observations	Status	Client's Action	Final Remark
1.1	Core <Automation Server> supports four security realms for authentication: delegate to servlet container; <Automation Server>'s own user database; LDAP; and Unix user/group database. (However there are many types of security realms extended through <Automation Server> plugins). Best authentication method is LDAP.				
2	**Authorization**				
2.1	Matrix based security allows user permissions configuration at a global level. Project-based matrix authorization strategy extends matrix- based security by allowing security on a per job basis. This option is beneficial for restricting access to jobs on a per group or user basis.				
3	**Access Control**				
3.1	Enable the slave to master access control. Because Master needs to temporarily take control of a user's machine to do a specific job. (Turn off this option if all nodes are under full control of the				

S. No.	Assessment Points	Observations	Status	Client's Action	Final Remark
	<Automation Server> master)				
4	**Enable SSL encryption**				
4.1	if <Automation Server> is running in standalone mode, encrypts all traffic between the browser and the <Automation Server> server. Self-signed SSL certificate will be fine.				
4.2	If client/server architecture is in use then trusted SSL from certified authority is required				
5	**Use a web server or a Winstone configuration file**				
5.1	<Automation Server> should not be run by executing java - jar from the command line. Specifying all parameters on the command line becomes a security risk because enabling SSL certificate requires exposing the keystore password in the parameter.				
5.2	Storing KeyStore password in a configuration file means not exposing passwords on the command line.				
5.3	Remove all permissions to the configuration file for group members' permission and other				

S. No.	Assessment Points	Observations	Status	Client's Action	Final Remark
	users' permission so that only the user who runs <Automation Server> master has access. This is a non- issue for web servers because they already utilize configuration files				
6	**Disable CLI**				
6.1	Best way to disable CLI is by placing a CLI shutdown script at $JENKINS_HOME/init.groovy.d				
6.2	Disable <Automation Server>'s sshd daemon. If required then it is recommended is to configure the sshd daemon to a known port so that firewall rules can whitelist <Automation Server> administrator's IP.				
7	**OS Hardening**				
7.1	It is necessary to harden the OS on which <Automation Server> is running.				
7.2	Install <Automation Server> with non GUI supportable OS. That will reduce attack surfaces				
7.3	Never run <Automation Server> with root/administrator privileges				

S. No.	Assessment Points	Observations	Status	Client's Action	Final Remark
7.4	Implement least privileges by removing sudoer access to the account that <Automation Server> uses.				
7.5	<Automation Server> master installed on Linux never need sudo access				
7.6	On Windows, make sure <Automation Server> user only belongs to "Users" group.				
7.7	Mac OS X should run <Automation Server> as "Standard User" because they are not allowed sudo access by default.				
7.8	The same rules (7.3 to 7.8) apply to <Automation Server> nodes because applications such as a compiler or automated testing run fine with non-administrator privileges				
7.9	Only open ports on the master are SSH, SSL/HTTP, and a pair of random ephemeral port if <Automation Server>' sshd daemon is enabled.				
8	**Apply OS Patches**				
8.1	Regularly applying system patches and OS updates				

S. No.	Assessment Points	Observations	Status	Client's Action	Final Remark
8.2	In addition to OS updates, updating Java is equally important because vulnerabilities in Java will put <Automation Server> at risk				
9	**Disabling unnecessary services. For example,** <Automation Server> master and its nodes do not need a file sharing service to function properly.				
10	**Protect Sensitive Files**				
10.1	If <Automation Server> uses Winstone, make sure winstone properties file is accessible only by the account running <Automation Server> because it contains KeyStore password.				
10.2	Make sure the configuration files are properly locked down by granting access only to the owner if running under web servers such as Tomcat or JBoss.				
10.3	SSL certificate file are properly locked down by granting access only to the owner				
10.4	Files resides in the folder pointing to JENKINS_HOME is accessible only				

S. No.	Assessment Points	Observations	Status	Client's Action	Final Remark
	by the account running <Automation Server> masters.				
11	**Application whitelisting and Antivirus**				
11.1	Application whitelisting is a necessity for hosts on which <Automation Server> master and nodes are running. Application should be from an approved list and deny everything else.				
11.2	Antivirus software is still essential for <Automation Server> master and nodes for fundamental protection against known virus and malware				
12	Turning on the host- based firewall on <Automation Server> servers and nodes is another layer of protection against attacks				

5.4 Findings of Docker

S. No.	Description	Device Setting	Status	Client's Action	Final Remarks
1	**Host Configuration**				
1.1	General Configuration				
1.1.1	Ensure that the version of Docker is up to date (Not Scored)				
1.2	**Linux Hosts Specific Configuration**				

S. No.	Description	Device Setting	Status	Client's Action	Final Remarks
1.2.1	Ensure a separate partition for containers has been created (Scored)				
1.2.2	Ensure only trusted users are allowed to control Docker daemon (Scored)				
1.2.3	Ensure auditing is configured for the Docker daemon (Scored)				
1.2.4	Ensure auditing is configured for Docker files and directories - /var/lib/docker (Scored)				
1.2.5	Ensure auditing is configured for Docker files and directories - /etc/docker (Scored)				
1.2.6	Ensure auditing is configured for Docker files and directories docker.service (Scored)				
1.2.7	Ensure auditing is configured for Docker files and directories docker.socket (Scored)				
1.2.8	Ensure auditing is configured for Docker files and directories - /etc/default/docker (Scored)				
1.2.9	Ensure auditing is configured for Docker files and directories /etc/sysconfig/docker (Scored)				

S. No.	Description	Device Setting	Status	Client's Action	Final Remarks
1.2.10	Ensure auditing is configured for Docker files and directories - /etc/docker/daemon.json (Scored)				
1.2.11	Ensure auditing is configured for Docker files and directories - /usr/bin/containerd (Scored)				
1.2.12	Ensure auditing is configured for Docker files and directories - /usr/sbin/runc (Scored)				
2	**Docker daemon configuration**				
2.1	Ensure network traffic is restricted between containers on the default bridge (Scored)				
2.2	Ensure the logging level is set to 'info' (Scored)				
2.3	Ensure Docker is allowed to make changes to iptables (Scored)				
2.4	Ensure insecure registries are not used (Scored)				
2.5	Ensure aufs storage driver is not used (Scored)				
2.6	Ensure TLS authentication for Docker daemon is configured (Scored)				
2.7	Enable user namespace support (Scored)				
2.8	Ensure the default c group usage has been confirmed (Scored)				

S. No.	Description	Device Setting	Status	Client's Action	Final Remarks
2.9	Ensure base device size is not changed until needed (Scored)				
2.10	Ensure that authorization for Docker client commands is enabled (Scored)				
2.11	Ensure centralized and remote logging is configured (Scored)				
2.12	Ensure live restore is enabled (Scored)				
2.14	Ensure Userland Proxy is Disabled (Scored)				
2.16	Ensure that experimental features are not implemented in production (Scored)				
2.17	Ensure containers are restricted from acquiring new privileges (Scored)				
3	**Docker daemon configuration files**				
3.1	Ensure that the docker.service file ownership is set to root:root (Scored)				
3.2	Ensure that docker.service file permissions are appropriately set (Scored)				
3.3	Ensure that docker.socket file ownership is set to root:root(Scored)				
3.4	Ensure that docker.socket file permissions are set to 644 or more restrictive (Scored)				

S. No.	Description	Device Setting	Status	Client's Action	Final Remarks
3.5	Ensure that the /etc/docker directory ownership is set to root:root (Scored)				
3.6	Ensure that /etc/docker directory permissions are set to 755 or more restrictively (Scored)				
3.7	Ensure that registry certificate file ownership is set to root:root (Scored)				
3.8	Ensure that registry certificate file permissions are set to 444 or more restrictively (Scored)				
3.9	Ensure that TLS CA certificate file ownership is set to root:root (Scored)				
3.10	Ensure that TLS CA certificate file permissions are set to 444 or more restrictively (Scored)				
3.11	Ensure that Docker server certificate file ownership is set to root:root (Scored)				
3.12	Ensure that the Docker server certificate file permissions are set to 444 or more restrictively (Scored)				
3.13	Ensure that the Docker server certificate key file ownership is set to root:root (Scored)				
3.14	Ensure that the Docker server certificate key file permissions are set to 400 (Scored)				

S. No.	Description	Device Setting	Status	Client's Action	Final Remarks
3.15	Ensure that the Docker socket file ownership is set to root:docker (Scored)				
3.16	Ensure that the Docker socket file permissions are set to 660 or more restrictively (Scored)				
3.17	Ensure that the daemon.json file ownership is set to root:root(Scored)				
3.18	Ensure that daemon.json file permissions are set to 644 or more restrictive (Scored)				
3.19	Ensure that the /etc/default/docker file ownership is set to root:root (Scored)				
3.20	Ensure that the /etc/sysconfig/docker file ownership is set to root:root (Scored)				
3.21	Ensure that the /etc/sysconfig/docker file permissions are to 644 or more restrictively (Scored)				
3.22	Ensure that the /etc/default/docker file permissions are set to 644 or more restrictively (Scored)				
4	**Container Images and Build File Configuration**				
4.1	Ensure that a user for the container has been created (Scored)				

S. No.	Description	Device Setting	Status	Client's Action	Final Remarks
4.2	Ensure Content trust for Docker is Enabled (Scored)				
4.3	Ensure that HEALTHCHECK instructions have been added to container images (Scored)				
5	**Container Runtime Configuration**				
5.1	Ensure that, if applicable, an AppArmor Profile is enabled (Scored)				
5.2	Ensure that, if applicable, SELinux security options are set (Scored)				
5.3	Ensure that Linux kernel capabilities are restricted within containers (Scored)				
5.4	Ensure that privileged containers are not used (Scored)				
5.5	Ensure sensitive host system directories are not mounted on containers (Scored)				
5.6	Ensure sshd is not run within containers (Scored)				
5.7	Ensure privileged ports are not mapped within containers (Scored)				
5.8	Ensure that the host's network namespace is not shared (Scored)				
5.9	Ensure that the memory usage for containers is limited (Scored)				

S. No.	Description	Device Setting	Status	Client's Action	Final Remarks
5.10	Ensure that CPU priority is set appropriately on containers (Scored)				
5.11	Ensure that the container's root filesystem is mounted as read only (Scored)				
5.12	Ensure that incoming container traffic is bound to a specific host interface (Scored)				
5.13	Ensure that the 'on-failure' container restart policy is set to '5' (Scored)				
5.14	Ensure that the host's process namespace is not shared(Scored)				
5.15	Ensure that the host's IPC namespace is not shared (Scored)				
5.16	Ensure mount propagation mode is not set to shared (Scored)				
5.17	Ensure that the host's UTS namespace is not shared (Scored)				
5.18	Ensure the default seccomp profile is not Disabled (Scored)				
5.19	Ensure that docker exec commands are not used with the privileged option (Scored)				
5.20	Ensure that cgroup usage is confirmed (Scored)				
5.21	Ensure that the container is restricted from acquiring additional privileges (Scored)				

S. No.	Description	Device Setting	Status	Client's Action	Final Remarks
5.22	Ensure that container health is checked at runtime (Scored)				
5.23	Ensure that the PIDs cgroup limit is used (Scored)				
5.24	Ensure that the host's user namespaces are not shared (Scored)				
5.25	Ensure that the Docker socket is not mounted inside any containers (Scored)				
6	**Docker Swarm Configuration**				
6.1.1	Ensure swarm mode is not Enabled, if not needed (Scored)				
6.1.2	Ensure that the minimum number of manager nodes have been created in a swarm (Scored)				
6.1.3	Ensure that swarm services are bound to a specific host interface (Scored)				
6.1.4	Ensure that all Docker swarm overlay networks are encrypted (Scored)				
6.1.5	Ensure that swarm manager is run in auto-lock mode (Scored)				
7	**Docker Enterprise Configuration**				
7.1	Universal Control Plane Configuration				
7.1.1	Configure the LDAP authentication service (Scored)	Docker Enterprise configuration is not used			
7.1.2	Use external certificates (Scored)	Docker Enterprise configuration is not used			

S. No.	Description	Device Setting	Status	Client's Action	Final Remarks
7.1.3	Enforce the use of client certificate bundles for unprivileged users (Not Scored)	Docker Enterprise configuration is not used			
7.1.4	Configure applicable cluster role-based access control policies (Not Scored)	Docker Enterprise configuration is not used			
7.1.5	Enable signed image enforcement (Scored)	Docker Enterprise configuration is not used			
71.6	Set the Per-User Session Limit to a value of '3' or lower(Scored)	Docker Enterprise configuration is not used			
7.1.7	Set the "Lifetime Minutes" and "Renewal Threshold Minutes" values to '15' or lower and '0' respectively (Scored)	Docker Enterprise configuration is not used			
7.2	**Docker Trusted Registry Configuration**				
7.2.1	Enable image vulnerability scanning (Scored)	Docker Enterprise configuration is not used			

5.5 Findings of Firewall

S. No.	Security Elements	Client's Comments	Observations	Status	Client's Action	Final Observation
1	**Reviewed Rule-sets:**					
	Anti-spoofing filters (blocked private addresses, internal addresses appearing from the outside)					
	User permit rules (e.g. allow HTTP to public web Server)					

S. No.	Security Elements	Client's Comments	Observations	Status	Client's Action	Final Observation
	Management permit rules (e.g. SNMP traps to network management server)					
	Noise drops (e.g. discard OSPF and HSRP chatter)					
	Deny and Alert (alert systems administrator about traffic that is suspicious)					
	Deny and log (log remaining traffic for analysis)					
2	**Reviewed Stateful Inspection**					
	Appropriate rules are set up in terms of source and destination IP's, source and destination ports and timeouts in state table.					
	The timeouts are appropriate so as not to give the hacker too much time to launch a successful attack.					
	If filtering on MAC addresses is allowed, review the filters to ensure that it is restricted to the appropriate MAC's as defined in the security policy.					
3	Reviewed Logging Logging is enabled and that the logs are reviewed to identify any potential patterns that could indicate an attack.					

S. No.	Security Elements	Client's Comments	Observations	Status	Client's Action	Final Observation
	Reviewed Patches and updates the latest patches and updates relating to firewall product is tested and installed					
4	If patches and updates are automatically downloaded from the vendors' websites, then update is received from a trusted site.					
	In the event that patches and updates are emailed to the systems administrator ensure that digital Signatures are used to verify the vendor and ensure that the information has not been modified en-route.					
	Location – DMZ					
5	Ensure that there are two firewalls – one to connect the web server to the internet and the other to connect the web server to the internal network.					
	In the event of two firewalls ensure that it is of different types and that dual NIC's are used. This would increase security since a hacker would need to have knowledge of the strengths, weaknesses and bugs of both firewalls					

S. No.	Security Elements	Client's Comments	Observations	Status	Client's Action	Final Observation
	The rule-sets for both firewalls would vary based on their location e.g. between web server and the internet and between web server and the internal network.					
6	Vulnerability assessments/ Testing Ascertain if there is a procedure to test for open ports using nmap and whether unnecessary ports are closed.					
	Ensure that there is a procedure to test the rule-sets when established or changed so as not to create a denial of service on the organization or allow any weaknesses to continue undetected.					
7	Compliance with security policy ensure that the rule set complies with the organization security policy.					

S. No.	Security Elements	Client's Comments	Observations	Status	Client's Action	Final Observation
8	Ensure that the following spoofed, private (RFC 1918) and illegal Addresses are blocked: Standard unroutables · 255.255.255.25 127.0.0.0 Private (RFC 1918) addresses ·10.0.0.0 – 10.255.255.255 · 172.16.0.0 – 172.31.255.255 · 192.168.0.0 - 192.168.255.25 5 Reserved addresses · 240.0.0.0 Illegal addresses · 0.0.0.0 UDP echo ICMP broadcast (RFC 2644)					
9	Ensure that loose source routing and strict source routing (lsrsr & ssrr) are blocked and logged by the firewall.					
10	Remote access If remote access is to be used, ensure that the SSH protocol (port 22) is used instead of Telnet.					
11	File Transfers If FTP is a requirement, ensure that the server, which supports FTP, is placed in a different subnet than the internal protected network.					

S. No.	Security Elements	Client's Comments	Observations	Status	Client's Action	Final Observation
12	Mail Traffic Ascertain which protocol is used for mail and ensure that there is a rule to block incoming mail traffic except to internal mail.					
13	ICMP (ICMP 8, 11, 3, 0) unreachable messages.					
14	IP Readdressing/IP Masquerading Ensure that the firewall rules have the readdressing option enabled such that internal IP addresses are not displayed to the external untrusted networks.					
15	Firewalls should be configured in failover mode					
16	Firewall management only using SSL/SSH.					
17	Password protection for the console access should be configured with enable password					
18	Idle SSH login connection time out set to 5 minutes					
19	Warning banner should be set "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.					

S. No.	Security Elements	Client's Comments	Observations	Status	Client's Action	Final Observation
	You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There					

Note: Findings related to ICS equipment like PLC, RTU, SCADA system may also be incorporated if the scope of VA includes the ICS systems. The TRF fields viz., Security Elements, Client's Comments, Observations Status, Client's Action and Final Observations will remain the same.

6.0 Approvals

Approved By: **Released**

By:

Date **Date**

SECTION 5

REQUIREMENTS FOR INSPECTION BODIES

1. Scope

The scope of this document is to define the attributes of a competent inspection body and the requirements pertaining to those attributes. The attributes include:

- General requirements include Impartiality, independence and Confidentiality Structural requirements, administrative requirements organization and management
- Resource requirements, personnel facilities and equipment
- Subcontracting
- Process requirements
- Inspection methods and procedures for handling inspection items and samples
- Inspection records
- Complaints and appeals process
- Management system requirements, documentation, records and control
- Management review, Internal audits, Corrective and Preventive actions

This set of requirements is interpreted when applied to IT and ICS sectors.
Note: Inspection activities can overlap with testing and certification activities where these activities have common characteristics. However, an important difference is that many types of inspection involve professional judgment to determine acceptability against general requirements, for which reason the inspection body needs the necessary competence to perform the task.

2. Requirements

2.1 The Inspection Bodies which are a part of the inspection scheme shall comply with the requirements specified in "**ISO/IEC 17020:2012 Conformity assessment — Requirements for the operation of various types of bodies performing inspection" and Additional, Refined, and Interpreted requirements for IT & OT systems & components 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 **'inspection process'**. This document shall be read in conjunction with the inspection process.

3. Guidance on the Requirements of ISO/IEC 17020:2012

3.1 The Board (AB) shall adopt the IAF Guidance on the application of ISO/IEC 17020:2012 as the requirement document of AB, whenever it is brought out. In the meantime, if any further clarifications beyond ISO/IEC 17020:2012 are required, the same will be issued by the Board on a case-to-case basis. The Board has decided not to specify any scope sectors for accreditation for this programme. The accreditation shall be granted as per ISO/IEC 17020:2012.

4. Accreditation Process

The interested Inspection Body shall apply to AB for accreditation in the prescribed format specifying the scope of Accreditation of the Inspection Body for:

- IT system and Infrastructure
- Industrial Control System and Infrastructure

Along with the application, the applicant encloses its documentation and internal DRR whereas the submissions are provided against each requirement of Annex A of this section. The applicant also provides the applicable fee and a declaration that all terms and conditions are abided.

The IBs are required to demonstrate that they have an experience of auditing minimum 2 clients (labs/facilities etc.) as per this inspection criteria so that AB has sufficient data to analyse that IBs have processes and capabilities in place to perform the inspection of the same effectively.

4.1 The secretariat of AB registers applications and informs the applicant. A six-step process is followed to complete the accreditation process.

4.1.1 Step 1 - Document Evaluation

The IB appoints a TL for this particular client applicant who is responsible for evaluating the documents and DRR where the applicant has submitted the conformity statements against each accreditation requirement. The TL cross-verifies these submissions with the documents and procedures/policies, as provided for their adequacies and completeness. If any gap is identified, the same is communicated to the IB. IB supplies the supplementary documentation to clarify the gap areas and if the fund is satisfactory, the TL recommends 'Step 2' which is a compliance assessment of IB.

4.1.2 Step 2 - Compliance Audit of Inspection Body

The accreditation body appoints an assessment team to check the conformity of the process and procedures of IB w.r.t the accreditation criteria mentioned in Annex A of this section. The assessment team take into cognisance the DRR and statement made by TL for addressal of all the criteria by IB. At this stage, the assessment team checks the implementation and effectiveness of policies and procedures. If during assessment any gap areas are identified, the same is communicated to the IB in the form of major/minor concerns. The IBs take the corrective and preventive action and inform the TL which are verified and if in compliance, an offline practical skill test is recommended to the AB.

4.1.3 Step 3 - Practical Skill Test

The organizations successful in Steps 1 and 2 are given two or more virtual images having applications/services installed with the known vulnerabilities and possible penetrations built for the offline in-house practical skills test, which they are required to test at their premises and submit the VA&PT report for the same. Participants must follow the instructions provided and can only submit reports in the provided template format. The organizations scoring 90% or above in the reports submitted by them are declared successful in Step 3 and eligible for the VA/PT practical skill test in Step 4. The organization will be given a maximum of two attempts to appear in offline PST. In case the organization is unsuccessful in qualifying at this stage even after two attempts, the organization may apply as a fresh applicant after a cooling period of one year from the date of the last test.

4.1.4 **Step 4 - Vulnerability Assessment/Penetration Testing Practical Skill Test (VA/PT PST)**

Different setups with different sets of vulnerabilities will be hosted in Test Beds and participant organizations are required to identify vulnerabilities and accomplish challenges in the assigned setup. Challenges will be declared in real time over the IRC channel to the participating organizations. Rule of Engagement (ROE) document along with the template for the post-exercise report will be provided to the eligible organization organizations by email. Organizations will be required to submit VA & PT reports to AB. Organizations scoring 90% or more will be considered for Step 5 i.e. Personal Interaction Session at NABAB. The organization will be given a maximum of two attempts to appear in VA/PT PST. In case the organization is unsuccessful in qualifying for VA/PT PST even after two attempts, the organization may apply as a fresh applicant after a cooling period of one year from the date of the last test.

4.1.5 **Step 5 - Personal Interaction Session**

For the purpose of a personal interaction session during the empanelment review process, a committee duly constituted by AB will interact with the applicant IB who has qualified in Step 4. The technical team of IB shall explain/ make a presentation on the interpretation of vulnerabilities and means of exploitation by the IB. A standard Test Bed will be provided. Each member of the Inspection Team will be tested for skill/competence for the scope.

4.1.6 **Step 6 – Grant of Accreditation**

An applicant IB clearing all the required steps 1 to 5 of accreditation, will be recommended for accreditation subject to background verification and clearance of the IB and its technical persons.

4.2 Maintenance of Accreditation

The IB shall demonstrate sustainable compliance with the accreditation requirements defined in Annex A of this section through annual surveillance visits by the AB. If any major NCs are found, the accreditation status may be suspended or cancelled. The IB shall fulfil their obligation for an annual fee, annual background verification, addressal of complaints and appeals and non-misuse of the Scheme Mark.

Annexure A

Requirement for Inspection Bodies

The requirements are adopted from ISO/IEC 17020:2017. The cyber security-specific requirements are prefixed with CS-IB in a row inserted without disturbing the content of ISO/IEC 17020:2017. Similarly, the requirements which are not applicable are tagged as *'Not Applicable'* in the row.

Clause no. of ISO 17020:2017	Requirement
4	**General requirements**
4.1	**Impartiality and independence (Refer Annex B of this section)**
4.1.1	Inspection activities shall be undertaken impartially.
4.1.2	The inspection body shall be responsible for the impartiality of its inspection activities and shall not allow commercial, financial or other pressures to compromise impartiality.
4.1.3	The inspection body shall identify risks to its impartiality on an ongoing basis. This shall include those risks that arise from its activities, or from its relationships, or from the relationships of its personnel. However, such relationships do not necessarily present an inspection body with a risk to impartiality.
4.1.4	If a risk to impartiality is identified, the inspection body shall be able to demonstrate how it eliminates or minimizes such risk.
4.1.5	The inspection body shall have top management commitment to impartiality.
4.1.6	The inspection body shall be independent to the extent that is required with regard to the conditions under which it performs its services. Depending on these conditions, it shall meet the minimum requirements stipulated in Annex A, as outlined below.
a)	An inspection body providing third-party inspections shall meet the type A requirements of Clause A.1 (third-party inspection body).
b)	An inspection body providing first-party inspections, second-party inspections, or both, which forms a separate and identifiable part of an organization involved in the design, manufacture, supply, installation, use or maintenance of the items it inspects and which supplies inspection services only to its parent organization (in-house inspection body) shall meet the type B requirements of Clause A.2.
	Not Applicable
c)	An inspection body providing first-party inspections, second-party inspections, or both, which forms an identifiable but not necessarily a separate part of an organization involved in the design, manufacture, supply, installation, use or maintenance of the items it inspects and which supplies inspection services to its parent organization or to other parties, or to both, shall meet the type C requirements of Clause A.3.
	Not Applicable
4.2	**Confidentiality**
4.2.1	The inspection body shall be responsible, through legally enforceable commitments, for the management of all information obtained or created during the performance of inspection activities. The inspection body shall inform the client, in advance, of the information it intends to place in the public domain. Except for information that the client makes publicly available, or when agreed between the inspection body and the client (e.g. for the purpose of responding to complaints), all other information is considered proprietary information and shall be regarded as confidential.

4.2.2	When the inspection body is required by law or authorized by contractual commitments to release confidential information, the client or individual concerned shall, unless prohibited by law, be notified of the information provided. Information about the client obtained from sources other than the client (e.g. complainant, regulators) shall be treated as confidential.
4.2.3	Information about the client obtained from sources other than the client (e.g. complainant, regulators) shall be treated as confidential.
5.	**Structural requirements**
5.1	**Administrative requirements**
5.1.1	The inspection 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 inspection activities.
5.1.2	An inspection body that is part of a legal entity involved in activities other than inspection shall be identifiable within that entity.
5.1.3	The inspection body shall have documentation which describes the activities for which it is competent.
CS-IB (IT)	The inspection bodies possess the necessary tools, skills, capabilities and procedures to carry out tasks such as: a. vulnerability assessment b. review of threat modeling and deployed architectures c. penetration testing d. IT security policy review and assessment against security best practices Information Security Testing e. Process Security Testing f. Internet Technology Security Testing g. Communications Security Testing h. Application security testing i. Wireless Security Testing j. Physical Security Testing to assess the security posture of IT systems and networks for protection against i. External threats, by way of remote infrastructure security assessment ii. Internal threats, by way of on-site infrastructure security assessment iii. Integrated system threats, by way of application security assessment
CS-IB (ICS)	The inspection bodies possess the necessary tools, skills, capabilities and procedures to carry out tasks as mentioned above in the ICS environment. Additionally, IB should have knowledge and skill to inspect/test/review/ architecture as per Purdue model or NIST 800-82, IIoT device inspection/testing, inspection as per the requirement of IEC 62443-3-2 and IEC 62443-3-3 (system security), capability to assess risk related with major accident (MA) and loss of essential services (LES) due to cyber breach. IB shall have knowledge to interpret FAT and SAT reports, documents, authorisations etc. and make use of the same for making the inspection plan and carry out the inspection.
5.1.4	The inspection body shall have adequate provisions (e.g. insurance or reserves) to cover liabilities arising from its operations.
5.1.5	The inspection body shall have documentation describing the contractual conditions under which it provides the inspection, except when it provides inspection services to the legal entity of which it is a part.

CS-IB (IT)	The IB shall agree to provide inspection services to the CSEs as per the requirements of inspection criteria of IT, the commercial contract to be entered into with the auditee organizations and abide by all the conditions of empanelment as well as service delivery.
CS-IB (ICS)	The IB shall agree to provide inspection services to the CSEs as per the requirements of inspection criteria of ICS, the commercial contract to be entered into with the auditee organizations and abide by all the conditions of empanelment as well as service delivery.
5.2	**Organization and management**
5.2.1	The inspection body shall be structured and managed so as to safeguard impartiality.
5.2.2	The inspection body shall be organized and managed so as to enable it to maintain the capability to perform its inspection activities.
5.2.3	The inspection body shall define and document the responsibilities and reporting structure of the organization.
5.2.4	Where the inspection body forms a part of a legal entity performing other activities, the relationship between these other activities and inspection activities shall be defined.
5.2.5	The inspection body shall have available one or more person(s) as technical manager(s) who have overall responsibility to ensure that the inspection activities are carried out in accordance with this International Standard.
NOTE	This person fulfilling this function does not always have the title of technical manager. The person(s) fulfilling this function shall be technically competent and experienced in the operation of the inspection body. Where the inspection body has more than one technical manager, the specific responsibilities of each manager shall be defined and documented.
5.2.6	The inspection body shall have one or more named person(s) who will deputize in the absence of any technical manager responsible for ongoing inspection activities.
5.2.7	The inspection body shall have a job description or other documentation for each position category within its organization involved in inspection activities.
CS-IB	The IB shall have procedure to make use of services of freelance consultants, consulting organisations and other expert groups to ensure that there is no conflict of interest and compromise on integrity and confidentiality of information.
6.	**Resource requirements**
6.1	**Personnel**
6.1.1	The inspection body shall define and document the competence requirements for all personnel involved in inspection activities, including requirements for education, training, technical knowledge, skills and experience.
Note	The competence requirements can be part of the job description or other documentation mentioned in 5.2.7.
CS-IB (IT)	Refer Annex D of Section 5: Requirements for Inspection Bodies. The IB shall have a procedure for police verification and background check for Inspectors in place.
CS-IB (ICS)	Refer Annex E of Section 5: Requirements for Inspection Bodies. The IB shall have a procedure for police verification and background check for Inspectors in place.

6.1.2	The inspection body shall employ, or have contracts with, a sufficient number of persons with the required competencies, including, where needed, the ability to make professional judgements, to perform the type, range and volume of its inspection activities.
6.1.3	The personnel responsible for inspection shall have appropriate qualifications, training, experience and a satisfactory knowledge of the requirements of the inspections to be carried out. They shall also have relevant knowledge of the following: a. the technology used for the manufacture of the products inspected, the operation of processes and the delivery of services; b. the way in which products are used, processes are operated and services are delivered; c. any defects which may occur during the use of the product, any failures in the operation of the process and any deficiencies in the delivery of services.
CS-IB (IT)	Refer Annex F of Section 5: Requirements for Inspection Bodies
CS-IB (ICS)	Refer Annex G of Section 5: Requirements for Inspection Bodies
6.1.4	They shall understand the significance of deviations found with regard to the normal use of the products, the operation of the processes and the delivery of services
CS-IB (IT)	Refer Annex F of Section 5: Requirements for Inspection Bodies
CS-IB (ICS)	Refer Annex G of Section 5: Requirements for Inspection Bodies
6.1.5	The inspection body shall have documented procedures for selecting, training, formally authorizing, and monitoring inspectors and other personnel involved in inspection activities
6.1.6	The documented procedures for training (see 6.1.5) shall address the following stages: an induction period; a mentored working period with experienced inspectors; continuing training to keep pace with developing technology and inspection methods.
6.1.7	The training required shall depend upon the ability, qualifications and experience of each inspector and other personnel involved in inspection activities, and upon the results of monitoring (see 6.1.8).
6.1.8	Personnel familiar with the inspection methods and procedures shall monitor all inspectors and other personnel involved in inspection activities for satisfactory performance. Results of monitoring shall be used as a means of identifying training needs (see 6.1.7).
6.1.9	Each inspector shall be observed on-site, unless there is sufficient supporting evidence that the inspector is continuing to perform competently
Note	It is expected that on-site observations are performed in a way that minimizes the disturbance of the inspections, especially from the client's viewpoint
6.1.10	The inspection body shall maintain records of monitoring, education, training, technical knowledge, skills, experience and authorization of each member of its personnel involved in inspection activities.
6.1.11	The personnel involved in inspection activities shall not be remunerated in a way that influences the results of inspections.
6.1.12	All personnel of the inspection body, either internal or external, that could influence the inspection activities shall act impartially.

6.1.13	All personnel of the inspection body, including sub-contractors, personnel of external bodies, and individuals acting on the inspection body's behalf, shall keep confidential all information obtained or created during the performance of the inspection activities, except as required by law.
CS-IB (IT)	The IB shall have a procedure for police verification/background check for Inspectors in place from applicable law enforcement bodies and records shall be maintained.
CS-IB (ICS)	The IB shall have a procedure for police verification/background check for Inspectors in place and records shall be maintained.
6.2	**Facilities and equipment**
6.2.1	The inspection body shall have available, suitable and adequate facilities and equipment to permit all activities associated with the inspection activities to be carried out in a competent and safe manner.
Note	The inspection body need not be the owner of the facilities or equipment that it uses. Facilities and equipment can be borrowed, rented, hired, leased or provided by another party (e.g. the manufacturer or installer of the equipment). However, the responsibility for the suitability and the calibration status of the equipment used in inspection, whether owned by the inspection body or not, lies solely with the inspection body.
6.2.2	The inspection body shall have rules for the access to, and the use of, specified facilities and equipment used to perform inspections.
6.2.3	The inspection body shall ensure the continued suitability of the facilities and the equipment mentioned in 6.2.1 for their intended use.
6.2.4	All equipment having a significant influence on the results of the inspection shall be defined and, where appropriate, uniquely identified.
6.2.5	All equipment (see 6.2.4) shall be maintained in accordance with documented procedures and instructions.
6.2.6	Where appropriate, measurement equipment having a significant influence on the results of the inspection shall be calibrated before being put into service, and thereafter calibrated according to an established programme.
6.2.7	The overall programme of calibration of equipment shall be designed and operated so as to ensure that, wherever applicable, measurements made by the inspection body are traceable to national or international standards of measurement, where available. Where traceability to national or international standards of measurement is not applicable, the inspection body shall maintain evidence of correlation or accuracy of inspection results.
6.2.8	Reference standards of measurement held by the inspection body shall be used for calibration only and for no other purpose. Reference standards of measurement shall be calibrated providing traceability to a national or international standard of measurement
CS-IB (IT) and CS-IB (ICS)	The IB shall have access to the Test Bed and a procedure to validate its integrity. They should document VA and PT procedures separately. They shall have technical documentation of the test bed. The IB shall have a plan for inter IB testing comparison to calibrate their own test beds and find out the standard deviation, if any and to bring within acceptable limits. IB shall have a test lab equipped with necessary test tools, test equipments, test

	environment including test bed supported by test methods, test engineers and analysts.
6.2.9	Where relevant, equipment shall be subjected to in-service checks between regular recalibrations.
	The testing tool shall be interpreted as equipment.
6.2.10	Reference materials shall, where possible, be traceable to national or international reference materials, where they exist.
	Not Applicable
6.2.11	Where relevant for the outcome of inspection activities, the inspection body shall have procedures for the following: • selection and approval of suppliers; • verification of incoming goods and services; • ensuring appropriate storage facilities.
6.2.12	Where applicable, the condition of stored items shall be assessed at appropriate intervals to detect deterioration.
6.2.13	If the inspection body uses computers or automated equipment in connection with inspections, it shall ensure that: computer software is adequate for use; Note: This can be done by the following: • validation of calculations before use; • periodic revalidation of related hardware and software; • revalidation whenever changes are made to related hardware or software; • software updates implemented as required. procedures are established and implemented for protecting the integrity and security of data; computer and automated equipment is maintained in order to ensure proper functioning.
6.2.14	The inspection body shall have documented procedures for dealing with defective equipment. Defective equipment shall be removed from service by segregation, prominent labeling or marking. The inspection body shall examine the effect of defects on previous inspections and, when necessary, take appropriate corrective action.
6.2.15	Relevant information on the equipment, including software, shall be recorded. This shall include identification and, where appropriate, information on calibration and maintenance.
6.3	**Subcontracting**

6.3.1	The inspection body shall itself normally perform the inspections that it contracts to undertake. Where an inspection body subcontracts any part of the inspection, it shall ensure and be able to demonstrate that the subcontractor is competent to perform the activities in question and, where applicable, complies with the relevant requirements stipulated in this International Standard or in other relevant conformity assessment standards. NOTE 1 Reasons to subcontract can include the following: an unforeseen or abnormal overload; key inspection staff members being incapacitated; key facilities or items of equipment being temporarily unfit for use; part of the contract from the client involving inspection not covered by the inspection body's scope or being beyond the capability or resources of the inspection body. NOTE 2 The terms “subcontracting” and “outsourcing” are considered to be synonyms. NOTE 3 Where the inspection body engages individuals or employees of other organizations to provide additional resources or expertise, these individuals are not considered to be subcontractors provided they are formally contracted to operate under the inspection body's management system (see 6.1.2).
6.3.2	The inspection body shall inform the client of its intention to subcontract any part of the inspection.
6.3.3	Whenever subcontractors carry out work that forms part of an inspection, the responsibility for any determination of conformity of the inspected item with the requirements shall remain with the inspection body.
6.3.4	The inspection body shall record and retain details of its investigation of the competence of its subcontractors and of their conformity with the applicable requirements of this International Standard or in other relevant conformity assessment standards. The inspection body shall maintain a register of all subcontractors
7.	**Process requirements**
7.1	**Inspection methods and procedures**
7.1.1	The inspection body shall use the methods and procedures for inspection which are defined in the requirements against which inspection is to be performed. Where these are not defined, the inspection body shall develop specific methods and procedures to be used (see 7.1.3). The inspection body shall inform the client if the inspection method proposed by the client is considered to be inappropriate. NOTE The requirements against which the inspection is performed are normally specified in regulations, standards or specifications, inspection schemes or contracts. Specifications can include client or in-house requirements.

CS-IB (IT) and CS-IB (ICS)	Inspection procedures shall be aligned in the following order: a. as prescribed by CIS b. as prescribed by OWASP c. as prescribed by NIST d. as prescribed by the component manufacturer/ vendor e. as per IB's own policy after consulting with CSEs
7.1.2	The inspection body shall have and shall use adequate documented instructions on inspection planning and on sampling and inspection techniques, where the absence of such instructions could jeopardize the effectiveness of the inspection process. Where applicable, the inspection body shall have sufficient knowledge of statistical techniques to ensure statistically sound sampling procedures and the correct processing and interpretation of results.
CS-IB (IT) and CS-IB (ICS)	The IB in consultation with the CSE shall identify the sample size as a part of inspection plan to get a reasonable degree of confidence that sample selected will represent the whole asset inventory. Each variant of the inventory shall represent in the sample. Generally, a 30% sample can be taken as a reference point and over a period of 3 years the whole population shall be covered.
7.1.3	When the inspection body has to use inspection methods or procedures which are non-standard, such methods and procedures shall be appropriate and fully documented. NOTE: A standard inspection method is one that has been published, for example, in international, regional or national standards, or by reputable technical organizations or by co-operation of several inspection bodies or in relevant scientific text or journals. This means that methods developed by any other means, including by the inspection body itself or by the client, are considered to be non-standard methods.
7.1.4	All instructions, standards or written procedures, worksheets, check lists and reference data relevant to the work of the inspection body shall be maintained up-to-date and be readily available to the personnel.
CS-IB (IT) and CS-IB (ICS)	Considerations should be given to: a. top 10 vulnerabilities published by OWASP every year b. NIST configuration checklist to build a library towards standardisation. c. FAT, SAT reports and documentation provided by OEMs
7.1.5	The inspection body shall have a contract or work order control system which ensures that: work to be undertaken is within its expertise and that the organization has adequate resources to meet the requirements; Note: Resources can include, but are not limited to, facilities, equipment, reference documentation, procedures or human resources. the requirements of those seeking the inspection body's services are adequately defined and that special conditions are understood, so that unambiguous instructions can be issued to personnel performing the duties to be required; work being undertaken is controlled by regular review and corrective action; the requirements of the contract or work order have been met.
7.1.6	When the inspection body uses information supplied by any other party as part of the inspection process, it shall verify the integrity of such information.
7.1.7	Observations or data obtained in the course of inspections shall be recorded in a timely manner so as to prevent loss of relevant information.

7.1.8	Calculations and data transfers shall be subject to appropriate checks. Note: Data can include textual material, digital data and anything else that is transferred from one location to another where errors could be introduced.
7.1.9	The inspection body shall have documented instructions for carrying out inspection in a safe manner.
7.2	**Handling inspection items and samples**
7.2.1	The inspection body shall ensure items and samples to be inspected are uniquely identified in order to avoid confusion regarding the identity of such items and samples.
7.2.2	The inspection body shall establish whether the item to be inspected has been prepared.
7.2.3	Any apparent abnormalities notified to, or noticed by, the inspector shall be recorded.
7.2.4	Where there is any doubt as to the item's suitability for the inspection to be carried out, or where the item does not conform to the description provided, the inspection body shall contact the client before proceeding.
7.2.5	The inspection body shall have documented procedures and appropriate facilities to avoid deterioration or damage to inspection items while under its responsibility.
7.3	**Inspection records**
7.3.1	The inspection body shall maintain a record system (see 8.4) to demonstrate the effective fulfilment of the inspection procedures and to enable an evaluation of the inspection.
7.3.2	The inspection report or certificate shall be internally traceable to the inspector(s) who performed the inspection.
7.4	**Inspection reports and inspection certificates**
7.4.1	The work carried out by the inspection body shall be covered by a retrievable inspection report or inspection certificate
7.4.2	Any inspection report/certificate shall include all of the following: a) identification of the issuing body; b) unique identification and date of issue; c) date(s) of inspection; d) identification of the item(s) inspected; e) signature or other indication of approval, by authorized personnel; f) a statement of conformity where applicable; g) the inspection results, except where detailed in accordance with 7.4.3. Note: Optional elements that can be included in inspection reports or certificates are listed in Annex C of this section.
CS-IB (IT)	For CII inspection reports, the requirements of Annex C of this section are mandatory and this annexure shall be treated as normative. Note: At present, the scheme doesn't have provision for inspection certificate.
CS-IB (ICS)	For CII inspection reports, the requirements of Annex C of this section are mandatory and this annexure shall be treated as normative. Note: At present, the scheme doesn't have provision for inspection certificate.

7.4.3	An inspection body shall issue an inspection certificate that does not include the inspection results [see 7.4.2 g)] only when the inspection body can also produce an inspection report containing the inspection results, and when both the inspection certificate and inspection report are traceable to each other.
CS-IB	This is not applicable at present.
7.4.4	All information listed in 7.4.2 shall be reported correctly, accurately, and clearly. Where the inspection report or inspection certificate contains results supplied by subcontractors, these results shall be clearly identified.
7.4.5	Corrections or additions to an inspection report or inspection certificate after issue shall be recorded in accordance with the relevant requirements of this subclause (7.4). An amended report or certificate shall identify the report or certificate replaced.
7.5	**Complaints and appeals**
7.5.1	The inspection body shall have a documented process to receive, evaluate and make decisions on complaints and appeals.
7.5.2	A description of the handling process for complaints and appeals shall be available to any interested party upon request.
7.5.3	Upon receipt of a complaint, the inspection body shall confirm whether the complaint relates to inspection activities for which it is responsible and, if so, shall deal with it.
7.5.4	The inspection body shall be responsible for all decisions at all levels of the handling process for complaints and appeals.
7.5.5	Investigation and decision on appeals shall not result in any discriminatory actions.
7.6	**Complaints and appeals process**
7.6.1	The handling process for complaints and appeals shall include at least the following elements and methods: a description of the process for receiving, validating, investigating the complaint or appeal, and deciding what actions are to be taken in response to it; tracking and recording complaints and appeals, including actions undertaken to resolve them; ensuring that any appropriate action is taken.
7.6.2	The inspection body receiving the complaint or appeal shall be responsible for gathering and verifying all necessary information to validate the complaint or appeal.
7,6,3	Whenever possible, the inspection body shall acknowledge receipt of the complaint or appeal, and shall provide the complainant or appellant with progress reports and the outcome.
7.6.4	The decision to be communicated to the complainant or appellant shall be made by, or reviewed and approved by, individual(s) not involved in the original inspection activities in question.
7.6.5	Whenever possible, the inspection body shall give formal notice of the end of the complaint and appeals handling process to the complainant or appellant.
8.	**Management system requirements**
8.1	**Options**

8.1.1	General The inspection body shall establish and maintain a management system that is capable of achieving the consistent fulfilment of the requirements of this International Standard in accordance with either Option A or Option B.
8.1.2	Option A The management system of the inspection body shall address the following: management system documentation (e.g. manual, policies, definition of responsibilities, see 8.2); control of documents (see 8.3); control of records (see 8.4); management review (see 8.5); internal audit (see 8.6); corrective actions (see 8.7); preventive actions (see 8.8); complaints and appeals (see 7.5 and 7.6).
8.1.2	Option B An inspection body that has established and maintains a management system, in accordance with the requirements of ISO 9001, and that is capable of supporting and
	demonstrating the consistent fulfilment of the requirements of this International Standard, fulfils the management system clause requirements (see 8.2 to 8.8).
8.2	**Management system documentation (Option A)**
8.2.1	The inspection body's top management shall establish, document, and maintain policies and objectives for fulfilment of this International Standard and shall ensure the policies and objectives are acknowledged and implemented at all levels of the inspection body's organization.
8.2.2	The top management shall provide evidence of its commitment to the development and implementation of the management system and its effectiveness in achieving consistent fulfilment of this International Standard.
8.2.3	The inspection body's top management shall appoint a member of management who, irrespective of other responsibilities, shall have responsibility and authority that include the following: ensuring that processes and procedures needed for the management system are established, implemented and maintained; and reporting to top management on the performance of the management system and any need for improvement.
8.2.4	All documentation, processes, systems, records, etc. related to the fulfilment of the requirements of this International Standard shall be included, referenced, or linked to documentation of the management system.
8.2.5	All personnel involved in inspection activities shall have access to the parts of the management system documentation and related information that are applicable to their responsibilities.
8.3	**Control of documents (Option A)**
8.3.1	The inspection body shall establish procedures to control the documents (internal and external) that relate to the fulfilment of this International Standard.

8.3.2	The procedures shall define the controls needed to: a) approve documents for adequacy prior to issue; b) review and update (as 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 apply suitable identification to them if they are retained for any purpose Note: Documentation can be in any form or type of medium, and includes proprietary and in-house developed software.
8.4	**Control of records (Option A)**
8.4.1	The inspection 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 International Standard.
8.4.2	The inspection 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.
8.5	**Management review (Option A)**
8.5.1	**General**
8.5.1.1	The inspection body's top management shall establish procedures to review its management system at planned intervals, in order to ensure its continuing suitability, adequacy and effectiveness, including the stated policies and objectives related to the fulfilment of this International Standard.
8.5.1.2	These reviews shall be conducted at least once a year. Alternatively, a complete review broken up into segments (a rolling review) shall be completed within a 12-month time frame.
8.5.1.3	Records of reviews shall be maintained.
8.5.2	Review inputs The input to the management review shall include information related to the following: a) results of internal and external audits; b) feedback from clients and interested parties related to the fulfilment of this International Standard. c) the status of preventive and corrective actions; d) follow-up actions from previous management reviews; e) the fulfilment of objectives; f) changes that could affect the management system; g) appeals and complaints.

8.5.3	Review outputs The outputs from the management review shall include decisions and actions related to: improvement of the effectiveness of the management system and its processes; improvement of the inspection body related to the fulfilment of this International Standard; resource needs.
8.6	**Internal audits (Option A)**
8.6.1	The inspection body shall establish procedures for internal audits to verify that it fulfils the requirements of this International Standard and that the management system is effectively implemented and maintained. Note: ISO 19011 provides guidelines for conducting internal audits.
8.6.2	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.
8.6.3	The inspection body shall conduct periodic internal audits covering all procedures in a planned and systematic manner, in order to verify that the management system is implemented and is effective.
8.6.4	Internal audits shall be performed at least once every 12 months. The frequency of internal audits may be adjusted depending on the demonstrable effectiveness of the management system and its proven stability.
8.6.5	The inspection body shall ensure that: a) internal audits are conducted by qualified personnel knowledgeable in inspection, auditing and the requirements of this International Standard; 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; f) the results of the audit are documented.
8.7	**Corrective actions (Option A)**
8.7.1	The inspection body shall establish procedures for identification and management of nonconformities in its operations.
8.7.2	The inspection body shall also, where necessary, take actions to eliminate the causes of nonconformities in order to prevent recurrence.
8.7.3	Corrective actions shall be appropriate to the impact of the problems encountered.
8.7.4	The procedures shall define requirements for the following: a) identifying nonconformities; b) determining the causes of nonconformity; c) correcting nonconformities; d) evaluating the need for actions to ensure that nonconformities do not recur; e) determining the actions needed and implementing them in a timely manner; f) recording the results of actions taken; g) reviewing the effectiveness of corrective actions.

8.8	**Preventive actions (Option A)**
8.8.1	The inspection body shall establish procedures for taking preventive actions to eliminate the causes of potential nonconformities.
8.8.2	Preventive actions taken shall be appropriate to the probable impact of the potential problems.
8.8.3	The procedures for preventive actions shall define requirements for the following: a) identifying potential nonconformities and their causes; b) evaluating the need for action to prevent the occurrence of nonconformities; c) determining and implementing the action needed; d) recording the results of actions taken; e) reviewing the effectiveness of the preventive actions taken. Note: The procedures for corrective and preventive actions do not necessarily have to be separate.

Annexure B
(normative)

Independence requirements for inspection bodies

A.1 Requirements for inspection bodies (Type A)

The inspection body referred to in 4.1.6 a) shall meet the requirements below.

a) The inspection body shall be independent of the parties involved.

b) The inspection body and its personnel shall not engage in any activities that may conflict with their independence of judgment and integrity in relation to their inspection activities. In particular, they shall not be engaged in the design, manufacture, supply, installation, purchase, ownership, use or maintenance of the items inspected.

NOTE 1 This does not preclude exchanging technical information between the client and the inspection body (e.g. explanation of findings, or clarifying requirements or training).

NOTE 2 This does not preclude the purchase, ownership or use of inspected items that are necessary for the operations of the inspection body, or the purchase, ownership or use of the items for personal purposes by the personnel.

c) An inspection body shall not be a part of a legal entity that is engaged in the design, manufacture, supply, installation, purchase, ownership, use or maintenance of the items inspected.

NOTE 1 This does not preclude exchanging technical information between the client and any other part of the same legal entity of which the inspection body is a part (e.g. explanation of findings, or clarifying requirements or training).

NOTE 2 This does not preclude the purchase, ownership, maintenance or use of inspected items that are necessary for the operations of another part of the same legal entity, or for personal purposes by the personnel.

d) The inspection body shall not be linked to a separate legal entity engaged in the design, manufacture, supply, installation, purchase, ownership, use or maintenance of the items inspected by the following:

i. common ownership, except where the owners have no ability to influence the outcome of an inspection;

EXAMPLE 1 A cooperative type of structure where there are large numbers of stakeholders, but they (individually or as a group) have no ability to influence the outcome of an inspection.

EXAMPLE 2 A holding company consisting of several separate legal entities (sister companies) under a common mother company, where neither the sister companies nor the mother company can influence the outcome of an inspection.

ii. common ownership appointees on the boards or equivalent of the organizations, except where these have functions that have no influence on the outcome of an inspection;

EXAMPLE A bank financing a company insists on an appointee to the board who will overview how the company is managed but will not be involved in any decision-making.

iii. directly reporting to the same higher level of management, except where this cannot influence the outcome of an inspection;

NOTE Reporting to the same higher level of management is permitted on matters other than design, manufacture, supply, installation, purchase, ownership, use or maintenance of the items inspected.

iv. contractual commitments, or other means that may have an ability to influence the outcome of an inspection.

Annexure C
(informative)

Optional elements of inspection reports and certificates

The following optional elements can be included in inspection reports and certificates:

a. designation of the document, i.e. as an inspection report or an inspection certificate, as appropriate;

b. identification of the client;

   Note: The owner of the inspected item can be mentioned in the report or certificate if the owner is not the client.

c. description of the inspection work ordered;

d. information on what has been omitted from the original scope of work;

e. identification or brief description of the inspection method(s) and procedure(s) used, mentioning the deviations from, additions to or exclusions from the agreed methods and procedures;

f. identification of equipment used for measuring/testing;

g. where applicable, and if not specified in the inspection method or procedure, reference to or description of the sampling method and information on where, when, how and by whom the samples were taken;

h. information on where the inspection was carried out;

i. information on environmental conditions during the inspection, if relevant;

j. a statement that the inspection results relate exclusively to the work ordered or the item(s) or the IoT inspected;

k. a statement that the inspection report should not be reproduced, except in full;

l. the inspector's mark or seal;

m. names (or unique identification) of the personnel members who have performed the inspection and, in cases when secure electronic authentication is not undertaken, their signature (see also 7.4.2).

   Note: Inspection certificate is not applicable at present.

Annexure D

Competence of Inspectors of IBs (IT)

Educational qualifications and experience of an inspector working in a IB is described below:

Parameters	Description
Educational Qualification	Graduate in computer science, computer engineering, telecommunication engineering, cyber security, electronics and information technology, instrumentation, software engineering, information systems etc.
Total experience (in IT) including cyber security	6 years in cyber security inspection
Professional experience in Industry/ Educational Institute	3 years
Inspection Experience	10 inspections of CII of various organisations
Experience in conducting Inspection/ VAPT/ IT Audits (in years)	3 years

Note: It is desirable that the VAPT engineer shall also have concepts of cyber security and experience in cyber security controls (e.g. ISO/IEC 27001:2022, NIST CSF, ICS) so that while analysing the test results, he is able to connect the effects of report findings of various controls.

Annexure E

Competence of Inspectors of IBs (ICS)

Educational qualifications and experience of an inspector working in a IB is described below:

Parameters	Description
Educational Qualification	Graduate in computer science, computer engineering, telecommunication engineering, cyber security, electronics and information technology, instrumentation, software engineering, information systems etc.
Total experience (in ICS) including cyber security	3 years
Total experience (in ICS and IT)	7 years
Professional experience in Industry/ Educational Institute	3 years
Inspection Experience	10 inspections of CII
Experience in conducting Inspection/ VAPT/ ICS infrastructure Audits (in years)	3 year by each inspector/test engineer

Annexure F

Training Requirements for IT Inspectors

1. Training acquired (minimum 24 hours) by an inspector working in an IB is described below:

a. The technology used for the manufacture of the products/infrastructure inspected, the operation of processes and the delivery of services;
b. The way in which products are used, processes are operated, and services are delivered;
c. Any defects/vulnerabilities which may occur during the use of the product, any failures in the operation of the process and any deficiencies in the delivery of services and its effect on the service continuity, and plant safety including risk of major accident and loss of essential services/functionalities.

2. Training on Inspection Criteria covering rationale of 18 controls, their applicability, inspection method and procedure, findings analysis and report preparations viz.:

a. Inventory and Control of Enterprise Assets
b. Inventory and Control of Software Assets
c. Data Protection
d. Secure Configuration of Enterprise Assets and Software
e. Account Management
f. Access Control Management
g. Continuous Vulnerability Management
h. Audit Log Management
i. Email and Web Browser Protections
j. Malware Defenses
k. Data Recovery
l. Network Infrastructure Management
m. Network Monitoring and Defense
n. Security Awareness and Skills Training
o. Service Provider Management
p. Application Software Security
q. Incident Response Management
r. Penetration Testing

Annexure G

Training Requirements for ICS Inspectors

1. Training acquired (minimum 24 hours) by an inspector working in an IB is described below:

a. The technology used for the manufacture of the products/infrastructure inspected, the operation of processes and the delivery of services;
b. The way in which products/components are used, processes are operated, and services are delivered;
c. Any defects/vulnerabilities which may occur during the use of the product, any failures in the operation of the process and any deficiencies in the delivery of services and its effect on the service continuity, and plant safety including risk of major accident and loss of essential services/functionalities.

2. Training on Inspection Criteria covering rationale of 20 controls, their applicability, inspection method and procedure, findings analysis and report preparations viz.:

a. Inventory and Control of Hardware Assets
b. Inventory and Control of Software Assets
c. Continuous Vulnerability Management
d. Control the use of administrative privileges
e. Secure Configurations for hardware and software on devices, laptops, workstations and servers
f. Maintenance, monitoring and analysis of audit norms
g. E-mail and web browser protection
h. Malware Defenses
i. Limitation and control of network ports, protocols and services
j. Data Recovery Capabilities
k. Secure Configurations for network devices such as firewalls, routers and switches
l. Boundary Defence
m. Data Protection
n. Controlled access based on need to know
o. Wireless access control
p. Account monitoring and control
q. Implement a security awareness and training programme
r. Application Software Security
s. Incident response and management
t. Penetration Tests and Red Team Exercise

SECTION 6

PROVISIONAL APPROVAL SYSTEM

1. Introduction

1.1. To operate inspection Scheme for CSEs hereafter referred to as **the Scheme**, Inspection Body (IB) shall need to primarily comply with the requirements specified in IB requirements under "**Conformity Assessment Framework for CSEs**" for obtaining accreditation from any AB which is a member of IAF.

1.2. For demonstrating compliance with the **inspection body requirements,** IBs are required to demonstrate that they have an experience of inspecting minimum 2 clients (labs/facilities etc.) as per this inspection criteria. There may be a situation where IB may not get a client for inspection, since in the beginning to get accreditation, they have to demonstrate their experience of inspection to the accreditation body and at the same time the client (CSEs) may not be willing to have a contract with unaccredited inspection bodies. As a result, IB may not be able to approach accreditation body (NABCB / any other IAF member accreditation body) 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 inspection 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 IBs are available at the beginning.

1.4. Therefore, it is necessary to establish a procedure for provisional approval of IBs under the Scheme till such time they can get formally accredited or get the accreditation scope extension from the NABCB / any other IAF member accreditation body and approved by the Scheme owner.

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

1.6. In order to be formally accredited by the NABCB **/** any other IAF member accreditation body, the IB, 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 Inspection 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 IB.

3. Scope

3.1. This document defines the procedure for IBs to obtain provisional approval to operate under the Scheme for Conformity Assessment Framework for CSEs, pending formal accreditation by NABCB / or any other AB which is signatory of IAF as per the prescribed requirements.

3.2. This approval shall be valid for a period of one year within which the provisionally approved IB would have to obtain formal accreditation by NABCB / or any other AB

which is signatory of IAF

3.3. This scope covers the inspection requirements as per the Inspection Criteria.

4. Objective

The objectives are to:

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

4.2. Demonstration of competencies by IB.

5. Requirement for Provisional Approval

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

5.1.2 Organisational Structure

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

5.2 Criteria

5.3

The potential IB shall be fully aware of the requirements of inspection and provisional approval including inspection 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 IB doesn't possess any experience in inspection but has the technical competence. They have a commitment to establish an IB for the applied scope.

5.2.2 IB 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 formalised the established processes.

5.2.3 IB operate in the IT sector (e.g. QMS) and intends to expand to ISMS and CSMS. In recent times, they have established the processes for the same.

For all the three scenarios, the IBs shall meet the technical criteria defined in this document, however they can conduct common audit if the CSE has opted for integrated management system.

5.4 The inspection body shall meet the following eligibility requirements

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

5.3.2. The IB shall have competency as per requirements of Annex D and E of 'Section 5: Requirements for Inspection Bodies'.

5.3.3. Acquired a complete understanding of the Inspection Criteria.

5.5 Integrity

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

5.6 Impartiality

5.2.1 The IB shall be impartial.

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

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

5.2.4 The IB shall act impartially in relation to its applicants, candidates and inspected CSEs.

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

5.2.6 The IB 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 IB by common ownership etc.

5.2.7 The IB 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 the applicant in the past.

5.3 Confidentiality

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

5.4 Safety and Security
The IB shall develop and document policies and procedures to ensure safety and security throughout the inspection process.

6. Inspection process

6.1 The IB shall manage the process of inspecting CSEs as per the documented 'Inspection Process' prescribed under the Scheme.

6.2 The IB shall maintain records to demonstrate that the inspection process is effectively implemented.

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

6.4 The IB shall certify CSEs only under the Scheme and shall use the logo of the Scheme in the SoC issued to the inspected CSEs.

6.5 The IB shall have written agreement with the inspected CSEs on the use of the SoC issued to them.

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

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

6.8 Contract agreement

The IBs shall have a legally enforceable agreement for the provision of inspection activities to CSEs. In addition, the IBs shall ensure its inspection agreement requires that the CSEs comply at least, with the specific requirements as prescribed in the relevant accreditation standards (ISO/IEC 17020:2017) and the Scheme document.

The contract agreement shall include the mechanism to handle inspected clients if IB does not extend approval or withdraws from accreditation.

6.9 Responsibility for decisions on SoC

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

6.10 Publicly available information

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

6.10.2 The IB shall maintain and make publicly available information describing its inspection processes for granting, maintaining, extending, renewing, reducing, suspending or withdrawing inspection, and about the inspection activities and geographical areas in which it operates.

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

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

7. Approval Process

Application

7.1 Any organization interested in approval as a IB 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 IB shall apply in the prescribe application form to the QCI for seeking provisional approval.

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

8.1.2 They shall have trained their auditors on technical aspects of the requirements of inspection criteria with desired competency.

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

8.2 On 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. 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 IB 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 inspection process by the applicant.

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

8.6 The date(s) of assessment shall be mutually agreed upon between the applicant IB 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 organization to assess its adequacy in line with the assessment criteria as specified. It will also involve verification of the implementation of the system including scrutiny of the records of personnel competence and other relevant records and 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.
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.

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 IB's competence.

9.3 The IB shall obtain formal accreditation as per the Inspection Scheme for IBs for its operation within one year of provisional approval by QCI.

9.4 Based on the request of the IB and review of previous performance, it may be decided to extend the period of validity; in such a case, the IB 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 IB 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 organization, 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 IB to fulfil the requirements for approval.

9.7 QCI shall examine such information and decide on the issue of its 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 IBs' Quality Assurance System (IB-QAS)

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

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

Note: If organisations have implemented ISO 9001 standards, the above requirements are deemed compliant.

B. Resource and Competence Requirements

The applicant IB 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 inspection criteria.

SECTION 7

RULES FOR USE OF SCHEME MARK

1. Introduction

1.1 The inspection scheme for Inspection Bodies is designed and developed as per international best practices.

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

1.3 The Mark is allowed to be used for promotion by accredited IBs, 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, 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 the use of the Scheme Mark.

3.2. This document sets out the conditions that must be followed by IBs 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 the 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 inspect IBs.

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 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 IBs 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 reinspection/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 Inspection Bodies.

7.3 The mark may also be used by the accredited IBs 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 “Inspection Process”.

7.11 Depending upon the degree of violation, suitable action(s) may range from advice for corrective actions, to withdrawal of inspection, 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 this document.

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

7.15 Misuse scenarios:

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

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

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

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

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- inspected, other than scope of Scheme, locations/personnel from offices are not included in scope or a related company are also inspected /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,) QCI (Scheme Manager), into disrepute.

9. Conditions for Use of the Scheme Mark by IBs

9.1 The Scheme Mark will be displayed only on the certificate issued to the clients of an accredited IB. 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 inspected, committing to the requirement of the Scheme through their IBs.

9.3 The IBs shall forward the filled contract form received from the inspected 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 inspections SoC granted – number, validity, etc.;

9.3.5 Scope of inspection 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 IBs 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 IBs.

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 IBs while issuing the statement of conformance.

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

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

Annexure A

Format for Application

APPLICATION FOR PERMISSION TO USE THE SCHEME MARK

1	**Name of the applicant IB**	
2	**Address**	
3	**Telephone No.**	
4	**Mobile No.**	
5	**Email**	
6	**Purpose of Usage**	
7	**Duration of Usage**	
8	**Inspection 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 IBs)

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 inspection status/ SoC 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 to 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 the 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 claims 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.

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 organization or an authorized signatory)

Title :

Address :

_____

Date : _____

Quality Council of India

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

Authorized Signatory: _____

Name : _____

Title : _____

Date : _____