Doc No: LITD 17(19143)

Preliminary Draft

Internet of Things Security & Privacy
Part 3: Assessment and Evaluation

ICS 35.030

BUREAU OF INDIAN STANDARDS

MANAKBHAVAN, 9 BAHADURSHAHZAFAR MARG NEW DELHI 110002

March 2022 Price Group

Table of Contents

1. *Introduction* 3
2. *Scope* 3
3. *Normative References* 3
4. *References* 3
5. *Acronyms* 3
6. *Definition* 3
7. *Compliance Process* 3

Bibliography **62**

1. Introduction

With enormous influx of IoT in our lifestyle (e.g. Smart City, Smart Traffic, Smart Metering, Telemedicine etc.), recent legal and regulatory requirements, new technologies with continuous evolving risk play a vital role in development of the "Internet of Things Security & Privacy" standard.

The assessment of Internet of Things is a way to identify the mistakes in application logic, configurations, implementation and deployment that jeopardize the security of IoT devices, networks, servers, web interfaces, mobile apps or data of IoT Ecosystem. While the requirements address the general practices that most organizations should take to secure their systems, some operational environments may present unique requirements which are not addressed here. IoT ecosystem should meet standardized as well as implied security as well as privacy requirements.

The security & privacy aspects of Internet of Things are covered in a set of documents having following parts, under the general title "Internet of Things Security & Privacy":

Part 1: Overview

Part 2: Controls and Requirements

Part 3: Assessment and Evaluation

The intent of this document is to provide the approach and methodology for assessment and evaluation of IoT Ecosystem and to list out a detailed compliance checklist.

2. Scope

This document provides the compliance process, approach and methodology for assessment and evaluation of Internet of Things with compliance checklist.

3. Normative References

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies:

- ISO/IEC 20924:2018 Information Technology – Internet of Things (IoT) - Vocabulary
- Doc No: LITD 17(19140) Internet of Things Security & Privacy - Part 1: Overview
- Doc No: LITD 17(19141) Internet of Things Security & Privacy - Part 2: Controls and Requirements

4. References

The following documents are adopted in this document:

- IoT Security Compliance Framework, Release 3.0, IoT Security Foundation, November 2021.

5. Acronyms

Acronyms given in Part 1 of this standard will apply.

6. Definition

Definitions given in Part 1 of this standard will apply.

7. Compliance Process

The compliance process includes the following steps:

- Conduct Risk Assessment of the Internet of Things in the target environment,
- Determine Assurance Level (as given in part 2) applicable to the IoT product,

- Conduct testing/audit for each requirement as per checklist given below for the determined assurance level for specified IoT product.

This document may be applied to individual IoT device or service of typical Internet of Things. The evaluation evidences for compliance should be recorded by the person performing testing/audit.

The checklist can also be used as a procurement mechanism to help specify requirements of a supplier contract. An organization procuring products, systems and services from a supplier may request testing/audit of the evidence.

A response to each requirement needs to be entered into Compliance Checklist, with supporting statements or evidence. For requirements deemed "not applicable", a justification for non-compliance or alternative countermeasures shall be provided.

Sl. No.	Applicability	Checkpoint	Method	Requirement Traceability
Control-01				
CP1.	IoT Service Provider	Ensure that the policy on data security defines level of security required internally and by the partner organizations on organization's data, their own data and customer's data.	Audit	SR1.
CP2.	IoT Service Provider	Ensure that IoT Service Provider have defined monitoring and logging policy that applies to various security classifications.	Audit	SR2.
CP3.	IoT Service Provider	Ensure that IoT Service Provider have defined incident management policy and all incidents related to physical security breach are handled accordingly.	Audit	SR3.
CP4.	IoT Service Provider/ Developer	Ensure that the exit procedure is defined for all stakeholders of IoT Ecosystem.	Audit	SR4.
CP5.	IoT Service Provider	Ensure that the policy and procedure for ownership change of IoT Ecosystem is defined.	Audit	SR5.
CP6.	IoT Service Provider	Ensure that the policy for enabling data review, transfer, sharing, disclosure, alteration and deletion is established and enforced.	Audit	SR6.
CP7.	IoT Service Provider	Ensure that the security update policy for low power IoT components are assessed to balance the needs of maintaining the	Audit	SR7.

		integrity and availability of IoT component.		
CP8.	IoT Service Provider	Ensure that a transparent and auditable policy is in place to update software/firmware of IoT components to fix any known vulnerability and notify respective users.	Audit	SR8.
CP9.	IoT Service Provider	Ensure that the policy for software update/patch is defined and enforced.	Audit	SR9.
CP10.	IoT Service Provider/ Developer	Ensure that the policy is established for interacting with the internal and third-party security researchers.	Audit	SR10.
CP11.	IoT Service Provider	Ensure that the policy is established for addressing risks that may impact security of the components incorporated into IoT Ecosystem.	Audit	SR11.
Control-02				
CP12.	Cloud	Ensure that the privileged roles are defined and implemented for any service/gateway that can configure devices.	Audit	SR12.
CP13.	IoT Service Provider	Ensure that the administrator role and authentication are separate for each component/tier in IoT Ecosystem.	Audit	SR13.
CP14.	IoT Service Provider	Ensure that management roles and responsibilities are defined in Information Security Incident Management Procedure to ensure effective and prompt resolution of information security incidents.	Audit	SR14.
CP15.	IoT Service Provider	Ensure that the security incident management process is applicable on all roles e.g. administrative employees, external consultants, vendor resources, visitors who have access to administrative information systems.	Audit	SR15.

CP16.	IoT Service Provider	Ensure that the responsibility is allocated for each stage of the update process involving controlling, logging and auditing of updates.	Audit	SR16.
CP17.	IoT Service Provider/ Developer	Ensure that the a person is nominated who takes ownership for adherence to this compliance checklist/certification process.	Audit	SR17.
CP18.	IoT Service Provider	Ensure that the role and responsibility for conducting awareness/training programs specific to IoT security/privacy are defined.	Audit	SR18.
Control-03				
CP19.	IoT device, IoT gateway	Ensure that the relationship between stakeholders, networks and IoT components are identifiable.	Audit	SR19.
CP20.	IoT Service Provider	Ensure that the software/firmware deployed on IoT devices and systems and their importance are identified and documented.	Audit	SR20.
CP21.	IoT Service Provider	Ensure that the mapping of cryptographic identities with chip identifiers is defined and backed up with IoT service provider.	Audit	SR21.
CP22.	IoT Service Provider	Ensure that IoT service provider defines the physical security perimeter for concerned department/facilities where information systems of IoT Ecosystem are deployed.	Audit	SR22.
CP23.	IoT Service Provider	Ensure that the physical access controls are imposed on perimeter of all facilities where information systems are hosted.	Audit	SR23.
CP24.	IoT Service Provider	Ensure that the list of all secure locations are maintained by the respective process owners for administrative purpose.	Audit	SR24.
CP25.	IoT Service Provider	Ensure that the serial numbers of all physical entities are recorded	Audit	SR25.

		during entry and exit of people from the premises.		
CP26.	IoT Service Provider	Ensure that the physical entities are tagged and the material coming in and going out are also tracked.	Audit	SR26.
CP27.	IoT Service Provider	Ensure that all information and data is adequately labelled and stored in separate safe locations.	Audit	SR27.
CP28.	Tag	Ensure that the access control measures are in place at critical physical entities to safeguard functioning of IoT Ecosystem.	Audit	SR28.
CP29.	Tag	Ensure that the perimeter of physical security are defined for organization/facilities/devices where components of IoT Ecosystem are deployed.	Audit	SR29.
Control-04				
CP30.	IoT Service Provider	Ensure that the security controls is imposed on offsite assets also.	Audit	SR30.
CP31.	Mobile Application	Ensure that all mobile devices and applications deployed in IoT Ecosystem are tested as per security requirements.	Audit	SR31.
CP32.	Mobile Application	Ensure that the mobile devices and applications are updated regularly.	Audit	SR32.
CP33.	Mobile Application	Ensure that the mobile application users are regularly informed about the potential threats.	Audit	SR33.
CP34.	Mobile Application	Ensure that the check for presence of baseline security controls on mobile device is performed by the mobile application related to IoT Ecosystem.	Audit	SR34.
CP35.	Mobile Application	Ensure that IoT Ecosystem does not communicate with unauthorized/modified/malicious mobile applications.	Audit	SR35.
CP36.	Mobile Application	Ensure that virus scans are done periodically without interfering with user's activities.	Audit	SR36.
CP37.	Mobile Application	Ensure that the mobile devices are controlled centrally to enable	Audit	SR37.

		ecosystem wide configurations, remote data management, remote data recovery and data wipe.		
CP38.	Mobile Application	Ensure that the mobile application ensures that any related databases or files are either tamper resistant or restricted in access.	Audit	SR38.
CP39.	Mobile Application	Ensure that the databases or files, are re-initialized upon detection of tampering.	Audit	SR39.
CP40.	Mobile Application	Ensure that the mobile device having access to databases and networks are disabled and users are alerted on detection of compromised device.	Audit	SR40.
CP41.	Mobile Application	Ensure that the white-list of suitable, applicable and safe applications are published and regularly updated within the organization and centrally imposed on all devices.	Audit	SR41.
CP42.	Mobile Application	Ensure that the mobile application follows OWASP Mobile Application Security Verification Standard.	Audit	SR42.
CP43.	Mobile Application	Ensure that the security checks or certificates are enforced in all mobile devices and applications.	Audit	SR43.
CP44.	Mobile Application	Ensure that the latest version of web browsers are used.	Audit	SR44.
Control-05				
CP45.	IoT device, IoT gateway, Servers	Ensure that the predefined secure revocation and decommissioning procedure is to be carried out on the end of life of IoT components.	Audit	SR45.
CP46.	IoT device, IoT gateway, Servers	Ensure that all items containing storage media are verified for sensitive data and licensed software is removed or securely overwritten prior to disposal or re-use.	Audit	SR46.
CP47.	IoT Service Provider/ Developer	Ensure that the IoT Service Provider/Developer provides	Audit	SR47.

		information about how removal or disposal of IoT device or service is to be carried out while maintaining the privacy and security.		
CP48.	IoT Service Provider	Ensure that IoT device or service have an irrevocable method of decommissioning/ recommissioning in case of ownership change.	Audit	SR48.
CP49.	IoT Service Provider	Ensure that the re-registration mechanism of IoT device or service with IoT Service Provider is secure.	Audit	SR49.
Control-06				
CP50.	IoT Service Provider	Ensure that IoT Ecosystem service Provider takes preventive and corrective actions in case of data breach by the partner to prevent future events.	Audit	SR50.
CP51.	IoT Service Provider	Ensure that IoT Ecosystem Service Provider is able to diagnose the source of the compromise, patch the system and deploy the patch on whole infrastructure.	Audit	SR51.
CP52.	IoT Service Provider	Ensure that the incident response policies and procedures are approved by competent authority of IoT Service provider to allow law enforcement.	Audit	SR52.
CP53.	IoT Service Provider	Ensure that the cybersecurity incident detection and prevention mechanism is implemented for timely detection and mitigation of information security incidents.	Audit	SR53.
CP54.	IoT Service Provider	Ensure that all information security incidents are recorded as per Information Security Incident Management Procedure.	Audit	SR54.
CP55.	IoT Service Provider	Ensure that the procedures are established for handling the different types of information security incidents.	Audit	SR55.

CP56.	IoT Service Provider	Ensure that malfunction or other abnormal system behavior is analyzed as potential information security incident.	Audit	SR56.
CP57.	IoT Service Provider	Ensure that all employees and third parties using administrative information systems and services report any observed or suspected information security weaknesses in systems or services.	Audit	SR57.
CP58.	IoT Service Provider	Ensure that all employees and third parties report the incidents to the designated point of contact as soon as possible in order to prevent further compromise.	Audit	SR58.
CP59.	IoT Service Provider	Ensure that the classification and prioritization of incidents is done to identify the impact and extent of damage.	Audit	SR59.
CP60.	IoT Service Provider	Ensure that all information security incidents are responded as per approved procedure or as directed by management.	Audit	SR60.
CP61.	IoT Service Provider	Ensure that the knowledge repository is referred for incident handling and as a source of learning for information security incidents.	Audit	SR61.
CP62.	IoT Service Provider	Ensure that the learnings from evaluation of information security incidents is communicated to all employees and follow-up action is taken against the responsible personnel based on evidences collected, maintained and presented to the relevant authorities.	Audit	SR62.
CP63.	Tag	Ensure that any incident related to malicious/abnormal usage of tags is handled as per incident management policy.	Audit	SR63.
Control-07				

CP64.	IoT device, IoT gateway	Ensure that the non-essential services of operating system are removed from the software, firmware or filesystem.	Audit	SR64.
CP65.	IoT device, IoT gateway	Ensure that the files, directories and persistent data are set to require minimum access privileges to correctly function.	Audit	SR65.
CP66.	IoT device, IoT gateway	Ensure that only necessary communication interfaces, network protocols, application protocols and network services are enabled.	Audit	SR66.
CP67.	IoT device, IoT gateway	Ensure that the applications do not require super user privileges under normal circumstances.	Audit	SR67.
CP68.	IoT device, IoT gateway	Ensure that the super-user privilege is dropped immediately after its use is over.	Audit	SR68.
CP69.	IoT device, IoT gateway	Ensure that the security or administration related processes are executed at higher privilege levels.	Audit	SR69.
CP70.	IoT device, IoT gateway	Ensure that the operating system kernel is designed such that each component runs with the minimal required capabilities.	Audit	SR70.
CP71.	IoT device, IoT gateway	Ensure that the IoT device or service have capability of generating random numbers using hardware or software based RNGs.	Audit	SR71.
CP72.	IoT device, IoT gateway	Ensure that the random number generator have the sufficient entropy source available.	Audit	SR72.
CP73.	IoT device, IoT gateway	If present, ensure that a true random number generator source have been validated for true randomness by Industry best practice certifications (e.g. NIST SP800-22, FIPS 140-2 or FIPS 140-3 or ISO/IEC 19790:2012 or ISO/IEC 24759:2017).	Audit	SR73.
CP74.	IoT device, IoT gateway	Ensure that the random number generator is used for all relevant	Audit	SR74.

		cryptographic operations e.g. generation of nonce, initialization vectors and keys.		
CP75.	IoT device, IoT gateway	Ensure that the IoT device or service have a validated hardware source for generating true random numbers.	Audit	SR75.
CP76.	IoT device, IoT gateway	Ensure that the IoT device or service have a very thin layer of secure bootloader and its integrity is verified first.	Testing	SR76.
CP77.	IoT device, IoT gateway	Ensure that the integrity of all configurations, signatures, public certificates and executables are cryptographically verified before their usage/execution.	Testing	SR77.
CP78.	IoT device, IoT gateway	Ensure that the secure boot loader is stored in a secure environment of executable memory, where it can be read, but not altered (e.g. internal ROM/lock-capable NVRAM/One Time Programmable Memory etc.).	Testing	SR78.
CP79.	IoT device, IoT gateway	Ensure that the secure bootloader does not allow external firmware/software to be loaded into memory for execution.	Testing	SR79.
CP80.	IoT device, IoT gateway	Ensure that the microprocessor/ microcontroller of IoT device or service is configured to execute secure bootloader first and then to load and execute subsequent firmware/software.	Testing	SR80.
CP81.	IoT device, IoT gateway	Ensure that the signature verification is performed using secure trust anchor.	Testing	SR81.
CP82.	IoT device, IoT gateway	Ensure that the default/factory bootloader is disabled or removed if it allows alternative images or firmware flashing.	Testing	SR82.
CP83.	IoT device, IoT gateway	Ensure that the control flow of IoT device or service ensures that any executable image can never be	Testing	SR83.

		loaded and executed without cryptographic verification of its integrity and authorization.		
CP84.	IoT device, IoT gateway	Ensure that the secure boot process is enabled by default and is not configurable.	Testing	SR84.
CP85.	IoT device, IoT gateway	Ensure that the IoT product have an irrevocable Hardware Secure Boot process.	Testing	SR85.
CP86.	IoT device, IoT gateway	Ensure that the IoT product have an irrevocable Hardware/Software Trusted root Secure Boot process.	Testing	SR86.
CP87.	IoT device, IoT gateway	Ensure that the IoT product have an irrevocable Hardware Trusted root Secure Boot process.	Testing	SR87.
CP88.	IoT device, IoT gateway	Ensure that the manifests containing firmware/software signing public key/signature are cryptographically verified against the root of trust.	Testing	SR88.
CP89.	IoT device, IoT gateway	Ensure that the firmware/software whitelisting is done.	Testing	SR89.
CP90.	IoT device, IoT gateway	Ensure that the IoT product have measures to prevent unauthenticated software and files from being loaded onto it. If the product is intended to allow unauthenticated software, Ensure that such software is only be run with limited permissions and/or sandbox.	Testing	SR90.
CP91.	IoT device, IoT gateway	Ensure that the operating system kernel and its functions are prevented from being called by external interfaces or unauthorized applications/emulators.	Testing	SR91.
CP92.	IoT device, IoT gateway	Ensure that the rogue or compromised applications are prevented from accessing areas of memory containing privileged resources such as TEE, trust anchor driver, hardware peripheral	Testing	SR92.

		registers or cryptographic parameters using memory protection techniques (e.g. Security Memory Protection Unit).		
CP93.	IoT device, IoT gateway	Ensure that the hardware fuses or immutable lock bits or software based locks are used for defining the protected memory areas.	Testing	SR93.
CP94.	IoT device, IoT gateway	Ensure that the memory is press-fitted or soldered on to the circuit board.	Testing	SR94.
CP95.	IoT device, IoT gateway	Ensure that the unencrypted sensitive data is cleared at the shutdown.	Testing	SR95.
CP96.	IoT device, IoT gateway	Ensure that the IoT service provider have catalogue of anomalies and baseline behavior list.	Audit	SR96.
CP97.	IoT device, IoT gateway	Ensure that the IoT service provider have the detailed anomalous behavior list readily available before supplying IoT device or service.	Audit	SR97.
CP98.	IoT device, IoT gateway	Ensure that the system watchdog timer is present and no provision is available to disable it.	Testing	SR98.
CP99.	IoT device, IoT gateway	Ensure that the level of tamper protection is based on the risk assessment.	Audit	SR99.
CP100.	IoT device, IoT gateway	Ensure that threat modelling and risk assessment is periodically conducted to analyse security threats to IoT Ecosystem.	Audit	SR100.
CP101.	IoT device, IoT gateway	Ensure that the risks categorized as medium or high are mitigated.	Audit	SR101.
CP102.	IoT Application	Ensure that the usage and lifecycle of critical security parameters are reviewed.	Testing	SR102.
CP103.	IoT Application	Ensure that the lifetime of sessions are optimally minimized, and automatic idle session logout is implemented.	Testing	SR103.

CP104.	IoT Application	Ensure that the IoT component have a secure source of time and its integrity is validated regularly.	Testing	SR104.
CP105.	IoT Application, Cloud/Server	Ensure that the cryptographic hash of password/pin with random salt value is used.	Audit	SR105.
CP106.	IoT Application, Cloud/Server	Ensure that the custom cryptographic algorithms (algorithms designed in-house) are not used.	Audit	SR106.
CP107.	IoT Application, Cloud/Server	Ensure that the use of insecure algorithms for cryptographic purposes is avoided.	Audit	SR107.
CP108.	IoT Application, Cloud/Server	Ensure that all keys are stored securely in accordance with Industry best practices (e.g. FIPS 140-2 or FIPS 140-3 or ISO/IEC 19790:2012).	Audit	SR108.
CP109.	Cloud/Server	Ensure that the all cipher suites are listed and validated against Industry best practices (e.g. NIST 800-131A, NIST SP 800-52 or OWASP).	Testing	SR109.
CP110.	Cloud	If run as a cloud service, ensure that the service complies to Industry standards, cloud security principles (e.g. Cloud Security Alliance, NIST Cyber Security Framework or UK Government Cloud Security Principles) and Indian Government regulations, policies and recommendations.	Audit	SR110.
CP111.	Mobile Application	Ensure that the official web pages are available only through secure connection.	Audit	SR111.
CP112.	Mobile Application	Ensure that the strict security measures are in place where there are high risks and highly sensitive data.	Audit	SR112.
CP113.	Cloud	Ensure that IoT Ecosystem's Cloud database is encrypted during storage and restricts read/write access to only authenticated and	Audit	SR113.

		authorized individuals, devices or services.		
CP114.	Cloud	Ensure that IoT Ecosystem's Cloud is designed using defence-in-depth architecture consisting of Virtual Private Cloud, firewalled access and cloud based monitoring.	Audit	SR114.
CP115.	Cloud/Server	Ensure that the IoT cloud service envisage the regulatory data protection capabilities e.g. isolation of tenant data, data privacy, data ownership, data localization, data lifecycle management, security authorization for data APIs etc.	Audit	SR115.
CP116.	Cloud, Server, Network	Ensure that all IoT Ecosystem related cloud, server and network elements have the latest operating system security updates implemented and processes shall be in place to keep them updated.	Audit	SR116.
CP117.	Cloud, Server, Network	Ensure that IoT Ecosystem's Cloud/server and network elements store any password using cryptographic implementation in line with Industry best practices (e.g. FIPS 140-2 or FIPS 140-3 or ISO/IEC 19790:2012).	Audit	SR117.
CP118.	Network	Ensure that the security is adequately analyzed before deciding telecommunication network for IoT Ecosystem.	Audit	SR118.
CP119.	Cloud/Server	Ensure that the server/database provisioning process involves security hardening.	Audit	SR119.
CP120.	IoT Application	Ensure that inputs in web applications are sanitized by using URL or HTML encoding to wrap data and treating it as literal text rather than executable code.	Audit	SR120.
CP121.	IoT Application	Ensure that all inputs and outputs are checked for validity using "Fuzzing" tests to check for	Audit	SR121.

		acceptable responses or output for both valid and invalid input stimuli.		
CP122.	IoT Application	Ensure that the data being transferred over internal interfaces is being validated.	Audit	SR122.
CP123.	IoT Service Provider/Developer	Ensure that cryptographic key chain used for signing production software/firmware is different from that used for any other test, development or other software image or support requirements.	Audit	SR123.
CP124.	IoT Service Provider/Developer	Ensure that IoT Service Provider follow Industry best practices (e.g. UK Cyber Essentials, NIST Cyber Security Framework, IS/ISO/IEC 27001) and minimum trustworthiness requirements related to security, safety, reliability, resilience and privacy as recommended by ISO/IEC, NIST, IIC and IISF.	Audit	SR124.
CP125.	IoT Service Provider/Developer	Ensure that IoT Service Provider define technical and business objectives for meeting the minimum security and trustworthiness levels, industrial and regulatory mandates, risk mitigations.	Audit	SR125.
CP126.	IoT device, IoT gateway	Ensure that all encryption keys are securely and truly randomly internally generated or securely programmed into each device as per Industry best Practices (e.g. FIPS 140-2 or FIPS 140-3 or ISO/IEC 19790:2012).	Audit	SR126.
Control-08				
CP127.	IoT device, IoT gateway	Ensure that the IoT component source code is written, reviewed, tested and maintained following the defined repeatable processes as language security standards (e.g. CERT, MISRA coding standards).	Audit	SR127.

CP128.	IoT device, IoT gateway	Ensure that the manual or tool based (SAST/DAST) secure code review is performed.	Audit	SR128.
CP129.	IoT device, IoT gateway	Ensure that the source code does not contain plaintext password or private key.	Audit	SR129.
CP130.	IoT device, IoT gateway	Ensure that the build environment and toolchain used to compile the application is run on build system with controlled and auditable access.	Audit	SR130.
CP131.	IoT device, IoT gateway	Ensure that the compiling process is hardened to restrict the potential vulnerabilities.	Audit	SR131.
CP132.	IoT device, IoT gateway	Ensure that the build environment and toolchain used to create the software is under configuration management system and gets validated regularly.	Audit	SR132.
CP133.	IoT device, IoT gateway	Ensure that the production build is compiled in such a way that all unnecessary debug/symbolic information is removed/disabled.	Audit	SR133.
CP134.	IoT device, IoT gateway	Ensure that the memory used for storage of sensitive contents (e.g. keys, passwords etc.) is cleared as soon as it is no longer needed.	Audit	SR134.
CP135.	IoT Application	Ensure that the inventory of third party or open source libraries used within IoT component are maintained with versions for keeping track of vulnerabilities and update requirements.	Testing	SR135.
CP136.	IoT Service Provider/Developer	Ensure that any hardware design file, software source code or final production software images with full descriptive annotations are stored encrypted in off-site locations or by 3rd party Escrow service.	Audit	SR136.
Control-09				
CP137.	Cloud/Server, Network	Where IoT Ecosystem includes any safety critical or life-impacting	Audit	SR137.

		functionality, ensure that the infrastructure incorporates protection against DDOS attacks, such as dropping of traffic or sink-holing as per Industry best practices e.g. NIST SP 800-53 SC-5.		
CP138.	Cloud/Server, Network	Where IoT Ecosystem includes any safety critical or life-impacting functionality, ensure that it has sufficient level of redundancy.	Audit	SR138.
CP139.	IoT Application	Ensure that the security and safety of IoT component and its connected components/users is not be compromised in case of unexpected/invalid inputs or erroneous software operation.	Audit	SR139.
CP140.	IoT Service Provider	Ensure that the procedure for safe evacuation of personnel is defined for emergency.	Audit	SR140.
CP141.	IoT Service Provider	Ensure that the escape directions are visibly posted throughout the premises.	Audit	SR141.
CP142.	IoT Service Provider	Ensure that the periodic emergency training and fire drills are conducted.	Audit	SR142.
Control-10				
CP143.	IoT device, IoT gateway	Ensure that the IoT component alerts the consumer/administrator on detection of tampering and not connect to wider networks than those necessary to perform the alerting function.	Audit	SR143.
CP144.	IoT device, IoT gateway, Web/Mobile Application	If a connection requires a password or passcode or passkey for connection authentication, ensure that the factory issued or reset password is unique to each IoT product.	Audit	SR144.
CP145.	IoT device, IoT gateway, Web/Mobile Application	Where a wireless interface has an initial pairing process, ensure that the passkeys are changed from the	Audit	SR145.

		factory issued, or reset password prior to providing normal service		
CP146.	IoT Application	Ensure that the administration interfaces are accessible only by authorized operators authenticated through mutual authentication mechanism.	Testing	SR146.
CP147.	Cloud/Server	Ensure that the internet facing systems have DDoS mitigation technique, load balancing systems, Redundant Systems and firewall in place.	Testing	SR147.
CP148.	Cloud/Server	Ensure that the same protection mechanism is in place in case of failure of firewall and other network protection systems as without any failure.	Audit	SR148.
CP149.	Cloud/Server	Ensure that the uncontrolled and any unintended packet forwarding functions are blocked.	Audit	SR149.
CP150.	Cloud/Server	Where webserver encrypts communication using TLS and requests a client certificate, ensure that certificate pinning is implemented.	Testing	SR150.
CP151.	Cloud/Server	Where webserver encrypts communication using TLS and requests a client certificate, ensure that the server only establishes a connection to IoT device or service if the client certificate and its trust chain is valid.	Testing	SR151.
CP152.	Cloud/Server	Ensure that the IoT product cloud/servers support appropriately secure TLS/DTLS ciphers and disable/remove support for deprecated ciphers as recommended by NIST SP 800-52, ENISA, SSL Labs, IETF RFC7525 and NCSC.	Audit	SR152.
CP153.	Cloud/Server	Ensure that the IoT Ecosystem server's TLS certificates are signed by trusted certification authorities;	Audit	SR153.

		are within their validity period; and processes are in place for their renewal.		
CP154.	Cloud/Server	Ensure that the IoT cloud/server have repeated renegotiation of TLS connections disabled.	Audit	SR154.
CP155.	Cloud/Server	Ensure that all IoT Ecosystem related servers shall have their webserver identification options, HTTP trace methods and unused ports disabled.	Testing	SR155.
CP156.	Cloud/Server	Ensure that all remote access to cloud/server shall be via secure means (e.g. SSH).	Audit	SR156.
CP157.	Cloud/Server	Ensure that the IoT Cloud/Server/ network elements only enable the communications interfaces, network protocols, application protocols and network services necessary for the operation.	Audit	SR157.
CP158.	Cloud/Server	Ensure that the deployed security/privacy mechanisms are consistent across web browsers, custom embedded devices or mobile applications.	Testing	SR158.
CP159.	Cloud/Server, Network	Ensure that IoT Ecosystem's Cloud/Server and network elements shall support access control measures to restrict access to sensitive information or system processes to privileged accounts.	Audit	SR159.
CP160.	Cloud/Server, Network	Ensure that IoT Ecosystem's Cloud/Server and network elements prevent anonymous/guest access except for read only access to public information.	Audit	SR160.
CP161.	Cloud/Server, Network	Ensure that TCP based communications are encrypted and authenticated using the latest Transport Layer Security standard.	Audit	SR161.
CP162.	Cloud/Server	Ensure that UDP based communications are encrypted	Audit	SR162.

		using the latest Datagram Transport Layer Security standard.		
CP163.	Cloud	Where the device identity and/or configuration registries are implemented within a cloud service, ensure that the registries are configured to restrict access to only authorised administrators.		SR163.
CP164.	Network	Ensure that IoT devices or services connect to cloud/servers using edge-to-cloud secure hardware (e.g. Zero Touch Provisioning).	Audit	SR164.
CP165.	Network	Ensure that secure channel is used for connecting to IoT Ecosystem through public WiFi networks.	Audit	SR165.
CP166.	Network	Ensure that Compartmentalization of system (e.g. network segmentation) is done.	Audit	SR166.
CP167.	Network	Ensure that IoT component use ephemeral identifiers to identify itself.	Audit	SR167.
CP168.	Network	Ensure that IoT components are securely authenticated before admitting them in IoT proximity network.	Audit	SR168.
CP169.	Network	Ensure that MAC addresses of IoT components are whitelisted so that only specified components can connect to WiFi network.	Audit	SR169.
CP170.	IoT gateway, IoT device, Network	Ensure that IoT components does not connect to a network, unless network supports secure protocols.	Audit	SR170.
CP171.	Cloud/Server	Ensure that APIs are implemented as per Industry best practices e.g. NIST SP 800, oneM2M TS-0003.	Audit	SR171.
CP172.	Cloud/Server	Ensure that services are allowed to access privileged resources only through constrained APIs.	Audit	SR172.
CP173.	Cloud/Server	Ensure that access to remote services and resources are verified by separate authentication tokens.	Audit	SR173.
CP174.	IoT Application	Ensure that the IoT Security policy related to encodings and characters	Audit	SR174.

		is enforced through sanitization APIs and raising of exceptions.		
CP175.	IoT Service Provider/Developer	Ensure that a securely controlled area and process is used for device provisioning, where the production facility is untrusted.	Audit	SR175.
Control-11				
CP176.	IoT device, IoT gateway	Ensure that the secure bootloader is audited for security by a third-party.	Testing	SR176.
CP177.	IoT device, IoT gateway	Ensure that the trust anchor is tamper-resistant and have appropriate certifications e.g. FIPS 140-2 or FIPS 140-3 or ISO/IEC 19790:2012.	Audit	SR177.
CP178.	IoT device, IoT gateway, Server, Cloud, API, Web Interface, Mobile Application	Ensure that the Vulnerability Assessment & Penetration Testing/Application Security Testing are conducted and no major issues are present before deployment of IoT components in IoT Ecosystem and its software updates.	Audit	SR178.
CP179.	IoT device, IoT gateway	Ensure that the independent verification of IoT components are carried out to ensure visibility and assurance of IoT Ecosystem adhering to stated cybersecurity objectives.	Audit	SR179.
CP180.	Cloud/Server	Ensure that the network component and firewall configurations are regularly reviewed and documented for the required/defined secure behavior.	Audit	SR180.
CP181.	Mobile Application	Ensure that the mobile application is free from OWASP Mobile Top 10 vulnerabilities.	Audit	SR181.
CP182.	IoT device, IoT gateway, Network	Ensure that the standardized and appropriate communication protocols are used and the implementation is certified.	Testing	SR182.
CP183.	IoT device, IoT gateway, Network	Ensure that the IoT component communication modules are	Testing	SR183.

		certified as per industry best practices.		
CP184.	IoT Service Provider	Ensure that the chip design is independently analysed and certified for security threats.	Audit	SR184.
CP185.	IoT Service Provider	Ensure that the process of loading executable image is defined, secure and auditable.	Audit	SR185.
CP186.	IoT Service Provider	Ensure that the executable image is verified before and after being flashed.	Audit	SR186.
CP187.	IoT Service Provider	Ensure that the process of provisioning cryptographic secrets is defined, secure and auditable.	Audit	SR187.
Control-12				
CP188.	IoT device, IoT gateway	Ensure that the IoT components log the pertinent details of cybersecurity events.	Audit	SR188.
CP189.	IoT device, IoT gateway	Ensure that the diagnostics information are also recorded at regular intervals and include as much environmental data (e.g. temperature, battery life, memory usage, execution time, process lists) of the IoT components as possible.	Audit	SR189.
CP190.	IoT device, IoT gateway	Ensure that the IoT service provider continually monitor the outliers and diagnose security and performance related problems in production environment.	Testing	SR190.
CP191.	IoT device, IoT gateway	Ensure that the back-end servers monitor the decommissioned/revoked IoT components and alert the user about its potential misuse.	Audit	SR191.
CP192.	Cloud/Server	Ensure that the IoT Ecosystem Service Provider have process to monitor the relevant security advisories to ensure all related web servers use protocols with no publicly known weaknesses.	Audit	SR192.

CP193.	Cloud/Server	Ensure that IoT Ecosystem's Cloud/Servers are monitored for compliance with connection policies and out-of-compliance connection attempts are reported.	Audit	SR193.
CP194.	Mobile Application	Ensure that organizations have mechanism in place to perform real time monitoring and to take necessary and immediate preventive actions.	Audit	SR194.
CP195.	Mobile Application	Ensure that the installation and use of mobile applications are restricted and monitored by the organization's internal policies and procedures.	Audit	SR195.
CP196.	Network	Ensure that the gateway is managed, monitored and updated.	Audit	SR196.
CP197.	Network	Ensure that link failure is monitored for potential security breach.	Audit	SR197.
CP198.	Cloud/Server	Ensure that the change of computing platform/location/SIM is being monitored.	Audit	SR198.
CP199.	IoT Service Provider	Ensure that administrators manage and monitor system parameters of IoT components (e.g. error, disk usage, bandwidth, memory and CPU utilization) and take corrective action.	Audit	SR199.
CP200.	IoT Service Provider	Ensure that IoT Ecosystem is monitored so that IoT Ecosystem service provider do not take actions for which they do not have user's consent.	Audit	SR200.
CP201.	IoT Service Provider/Developer	In manufacturing/provisioning, ensure that all devices are logged by the IoT Service Provider/Developer, utilising unique tamper resistant identifiers, so that cloned or duplicated devices can be identified and disabled or prevented from being used within IoT Ecosystem.	Audit	SR201.

CP202.	IoT Service Provider/Developer	Ensure that the production system for a device have a process to ensure that any device with duplicate serial numbers are not shipped and are either reprogrammed or destroyed.	Audit	SR202.
CP203.	IoT Service Provider	Ensure that the logs of network, application, system, database and cybersecurity incidents are maintained.	Audit	SR203.
CP204.	IoT Service Provider	Ensure that the events related to user authentication, management of accounts and access rights, modification of security rules and operations of the IoT Ecosystem are logged.	Audit	SR204.
CP205.	IoT Service Provider	Ensure that IoT Ecosystem is monitored on real-time basis to detect anomalies, excess radio interfaces or erroneous network traffic.	Audit	SR205.
CP206.	IoT Service Provider	Ensure that IoT Ecosystem service provider utilizes partner enhanced monitoring to limit exposures.	Audit	SR206.
CP207.	IoT Service Provider	Ensure that the detailed log is maintained for forensic analysis.	Audit	SR207.
CP208.	IoT Service Provider	Ensure that the restricted zones have adequate environment protection measures, including fire detection and extinguishing system, Humidity & Temperature indicator, raised flooring.	Audit	SR208.
CP209.	IoT Service Provider	Ensure that the equipment calibration/maintenance procedure/ schedule/records is maintained.	Audit	SR209.
CP210.	Tag	Ensure that the list of tags are maintained and monitored.	Audit	SR210.
Control-13				
CP211.	IoT device, IoT gateway	Ensure that the IoT components make logs accessible to authorized users and systems through secure login/log shipping mechanisms.	Audit	SR211.

CP212.	IoT device, IoT gateway	Ensure that the logs are protected against destruction and unintended alteration.	Audit	SR212.
CP213.	IoT Service Provider	Ensure that the logs are backed up on persistent read only storage in encrypted format and retrievable via authenticated connections.	Audit	SR213.
CP214.	IoT device, IoT gateway	Ensure that the enclosure of IoT device/gateway is tamper resistant.	Audit	SR214.
CP215.	IoT device, IoT gateway	Ensure that the sensitive contents in memory like RAM, Flash, are deleted on detection of tampering.	Audit	SR215.
CP216.	IoT device, IoT gateway	Ensure that the tamper evident measures are available in IoT component to indicate any tampering attempt.	Audit	SR216.
CP217.	IoT device, IoT gateway	Ensure that the IoT device/gateway incorporates physical protections against reverse engineering.	Audit	SR217.
Control-14				
CP218.	IoT device, IoT gateway	Ensure that the sufficiently secure communication channel is used between the programming/provisioning facility and the manufacturer for provisioning identity in IoT components.	Audit	SR218.
CP219.	IoT device, IoT gateway	Ensure that the remote administration of IoT components are via secure communication channel.	Testing	SR219.
CP220.	IoT device, IoT gateway, Network	Ensure that the sensitive data transmitted over communication channels are secured using encryption techniques in line with industry best practices.	Testing	SR220.
CP221.	IoT device, IoT gateway, Network	Ensure that the integrity verification mechanisms are used for messages exchanged between peer IoT components.	Testing	SR221.
CP222.	IoT device, IoT gateway, Network	Ensure that the communication channel uses physical layer security mechanisms for networks.	Testing	SR222.

CP223.	IoT device, IoT gateway, Network	Ensure that the ephemeral asymmetric/symmetric keys are used during key negotiation process.	Testing	SR223.
CP224.	IoT device, IoT gateway, Network	Ensure that the encryption is adequate for lightweight IoT component, network and the service being provided.	Testing	SR224.
CP225.	IoT device, IoT gateway, Network	Ensure that the Network operators provide and manage secure connections to IoT private networks using Virtual Private Network.	Testing	SR225.
CP226.	Network	Ensure that the network have necessary geographically distributed redundancy and isolation.	Audit	SR226.
CP227.	Network	Ensure that the IoT component remain operating and locally functional in case of loss of network connection and recover securely and safely in case of restoration of power.	Audit	SR227.
CP228.	Network	Ensure that IoT components return to a network in an orderly fashion, rather than in massive reconnection attempts.	Audit	SR228.
CP229.	Network	Ensure that the secure route establishment, automatic secure recovery and stabilization, malicious node detection, lightweight or hardware-supported computations and node location privacy functionalities are available in telecommunication network.	Audit	SR229.
CP230.	Network	Ensure that the encryption at the service layer is performed while using USSD, SMS or GPRS communication system in IoT Ecosystem.	Audit	SR230.
CP231.	Network	Ensure that the organizations restrict IoT components that are	Audit	SR231.

		allowed to connect to private network of IoT Ecosystem over cellular network using secure private APN.		
CP232.	Network	Ensure that the timestamp and nonce are included in 6LoWPAN messages.	Audit	SR232.
CP233.	Network	Ensure that the hash chains are used and purging of messages from suspicious senders are done.	Audit	SR233.
CP234.	Network	Ensure that the IoT components, subscribers and network providers are securely authenticated.	Audit	SR234.
CP235.	Network	Ensure that HLR and VLR are protected against Denial of Service attacks.	Audit	SR235.
CP236.	Network	Ensure that the network access is restricted to IoT components configured for Extended Access Barring in addition to common and domain-specific access control mechanisms.	Audit	SR236.
CP237.	Network	Ensure that Network security gateways have "sinkhole" for Denial of Service attacks.	Audit	SR237.
CP238.	Network	Ensure that the critical IoT components are identified and provided distinguished network services.	Audit	SR238.
CP239.	Network	Ensure that the registration of roaming IoT components are restricted for 'low priority' devices and allowed for 'high priority' devices under signalling storm conditions.	Audit	SR239.
CP240.	Network	Ensure that the messages from unauthorized/fake home networks/roaming partners are blocked either by changing communication profile of the IoT components or by enforcing stringent security policies.	Audit	SR240.

CP241.	Network	Ensure that secure protocols are used for interconnection of gateway to network backbone.	Audit	SR241.
CP242.	Network	Ensure that network operators implement localized "grey listing" of IoT components to temporarily block malicious nodes. The "black listing" of IoT components are done on confirmation of malicious behavior. For critical services, the blocking of IoT components are avoided.	Audit	SR242.
CP243.	Network	Ensure that the IoT component with IMEI support device host identity reporting.	Audit	SR243.
CP244.	Network	Ensure that backup channels are available in case of physical or logical link failure.	Audit	SR244.
CP245.	Network	Ensure that management of SIM is securely done.	Audit	SR245.
CP246.	Network	Ensure that network security related to regulatory requirements is managed.	Audit	SR246.
CP247.	Network	Ensure that communication options are set to minimum for IoT Ecosystem.	Audit	SR247.
CP248.	Network	Ensure that the wireless communication is sufficiently secure.	Audit	SR248.
CP249.	Network	Ensure that WPA2 WPS, if present, have unique, random key per device and enforce exponentially increasing retry attempt delays.	Audit	SR249.
CP250.	Network	Ensure that the routers with hardware based firewall are used in IoT Ecosystem.	Audit	SR250.
CP251.	Network	Ensure that the production components are protected using regularly updated end point protection solutions.	Audit	SR251.
CP252.	Network	Ensure that the wireless router's range is configured to cover only the intended area.	Audit	SR252.

Control-15				
CP253.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that additional protection mechanisms are implemented, where Universal Plug and Play (UPnP) protocol is enabled.	Testing	SR253.
CP254.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that physical reset button is not present in unattended IoT device or service.	Testing	SR254.
CP255.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the development, testing, debugging or diagnostics ports/configurations/login accounts are securely disabled/removed in production environment.	Audit	SR255.
CP256.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the debugging ports (e.g. JTAG and SWD) are disabled by altering security fuses or locks.	Audit	SR256.
CP257.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the port input commands are deactivated and the response of command does not provide any information regarding credentials, memory address or function names, where a port is used for field diagnostics,	Testing	SR257.
CP258.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the microcontroller/ microprocessor does not allow firmware/software to be read out of non-volatile memory in production devices.	Testing	SR258.
CP259.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the memory contents are encrypted where external non-volatile memory is used.	Testing	SR259.
CP260.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the IoT Ecosystem components have correct time source and the time sync is happening without error.	Testing	SR260.
CP261.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the configuration of IoT device or service is tamper resistant i.e. sensitive configuration	Audit	SR261.

		parameters should be changeable by authorised people only.		
CP262.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the configuration is provisioned to the device or service just in time by authorised services, to replace any existing pre-configuration for secure operation.	Audit	SR262.
CP263.	Cloud/Server	Ensure that the ingress and egress filtering mechanisms are defined/enabled in firewall or network traffic rulesets before any service is offered to public.	Audit	SR263.
CP264.	Network	Ensure that the remote changes of router settings over the Internet is disabled.	Audit	SR264.
CP265.	Network	Ensure that the router's default settings and names are changed.	Audit	SR265.
CP266.	Cloud/Server	Ensure that the secure server provisioning process is used that defines, configures, personalizes, and deploys a server in the production environment.	Audit	SR266.
CP267.	Cloud/Server	Ensure that APIs do not expose critical security parameters to an insecure application or hardware environment.	Audit	SR267.
CP268.	Cloud	Ensure that IoT Ecosystem's Cloud service binds API keys to specific IoT applications and are not installed on non-authorised devices.	Audit	SR268.
CP269.	Cloud	Ensure that IoT Ecosystem's Cloud service API Keys are not be hardcoded into devices or applications.	Audit	SR269.
CP270.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the ports, which are not used as part of normal operation, are not physically/logically accessible or communicate only with authorized and authenticated entities.	Testing	SR270.
CP271.	IoT Service Provider/Developer	Ensure that the IoT product allows the factory issued or OEM login accounts to be disabled or erased or renamed when installed or commissioned.	Audit	SR271.

CP272.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that users are provided guidance on changing the default password/username during the initial setup of IoT device or service.	Testing	SR272.
Control-16				
CP273.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the user is locked out pending multi-factor authentication after the threshold login attempts are reached.	Testing	SR273.
CP274.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the administrative cryptographic keys/passwords are unique and separate for each IoT component.	Testing	SR274.
CP275.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the multi-factor authentication is enforced for remote administration.	Testing	SR275.
CP276.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the remote administration capabilities are not available to publicly accessible applications or APIs.	Testing	SR276.
CP277.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the IoT components are protected against the replay of remote administration commands.	Testing	SR277.
CP278.	Cloud/Server, Network	Ensure that all cloud/servers and network elements enforce passwords that follows Password policy.	Audit	SR278.
CP279.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that cloud/server subsystem allow IoT components to join and leave the network as long as the IoT components are able to cryptographically prove their identity.	Testing	SR279.
CP280.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that cloud/server subsystem and IoT component implement mutual authentication.	Testing	SR280.
CP281.	IoT device, IoT gateway, cloud,	Ensure that each peer in IoT ecosystem authenticate all other	Testing	SR281.

	Web/Mobile Application	peers that participate in the IoT ecosystem.		
CP282.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that each peer signs messages sent to other peers in the network.	Testing	SR282.
CP283.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that each peer that receives a message cryptographically validates it prior to acting on it.	Testing	SR283.
CP284.	Cloud/Server	Ensure that IoT device or service authenticates users with backend authorizations or local passcodes.	Audit	SR284.
CP285.	Cloud/Server	Ensure that Central Authentication Service first authenticate the user to local application, then enforce policies and procedures that ensure how authentication token can be used and for what period of time.	Audit	SR285.
CP286.	Cloud/Server	Ensure that the token is invalidated on detection of abnormal behaviour and the user is forced to log in back using multi-factor authentication.	Audit	SR286.
CP287.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the implemented authentication mechanism cannot be bypassed, tampered, or falsified.	Audit	SR287.
CP288.	IoT Service Provider	Ensure that there is provision for multifactor authentication for ensuring enhanced security.	Audit	SR288.
CP289.	IoT Service Provider	Ensure that administration interfaces are accessible only by authorized operators who are authenticated through mutual & multifactor authentication mechanisms.	Audit	SR289.
Control-17				
CP290.	IoT device, IoT gateway, Web/Mobile Application	Where remote software updates are supported by IoT product, ensure that the software/firmware images are digitally signed by an appropriate signing authority - e.g.	Audit	SR290.

		manufacturer/supplier or public, and are identified.		
CP291.	IoT device, IoT gateway, Web/Mobile Application	Where updates are supported, ensure that the software update package have its digital signature, signing certificate and signing certificate chain verified by the IoT product before the update process begins.	Audit	SR291.
CP292.	IoT device, IoT gateway	Where IoT product cannot verify authenticity of updates itself (e.g. due to no cryptographic capabilities), ensure that only a local update by a physically present user is permitted and is their responsibility.	Audit	SR292.
CP293.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the software signing key for each update image is uniquely generated.	Audit	SR293.
CP294.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the signed update image, signature, public key for next update is made available through secure update mechanism or service.	Audit	SR294.
CP295.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the update are performed over encrypted communication channel when updates are conducted over the air (OTA).	Audit	SR295.
CP296.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the IoT component authenticates the peer before accepting the update.	Testing	SR296.
CP297.	IoT device, IoT gateway	Ensure that the support for partially installing updates are available for constrained IoT products whose on-time is insufficient for the complete installation of a whole update.	Audit	SR297.
CP298.	IoT device, IoT gateway	Ensure that the support for partially downloading updates are available	Audit	SR298.

		for IoT products whose network access is limited or sporadic.		
CP299.	IoT device, IoT gateway, cloud, Web/Mobile Application	Where real-time expectations of performance are present, ensure that the update mechanisms not interfere with meeting these expectations.	Testing	SR299.
CP300.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the user data/credentials are re-initialized upon firmware/software update, if secure update/boot is not supported.	Testing	SR300.
CP301.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the IoT product is able to revert to the recoverable state, if update process fails.	Testing	SR301.
CP302.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the IoT product is not performing operations until update is fully applied or fully reverted.	Audit	SR302.
CP303.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the IoT device or service rolls back to last known good configuration that was stored on the device, if authenticity of update could not be verified.	Audit	SR303.
CP304.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the cryptographic keys for updates are securely provisioned during manufacturing/secure update as per Industry best practices e.g. FIPS 140-2 or FIPS 140-3 or ISO/IEC 19790:2012.	Audit	SR304.
CP305.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the IoT device or service is always able to connect to the update server for downloading the updates, if update process fails.	Audit	SR305.
CP306.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the IoT device or service is always able connect to the backend for submitting diagnostics information in case of update process failure.	Audit	SR306.
CP307.	IoT device, IoT gateway, cloud,	Ensure that the IoT device or service have the protection	Audit	SR307.

	Web/Mobile Application	mechanisms against unauthorized reversion of firmware/software to an earlier version.		
CP308.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the IoT device or service allows authorized reversion of firmware/software to an earlier version in case of failed updates.	Audit	SR308.
CP309.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the secure backup for the active application images are kept by the IoT Service Provider.	Audit	SR309.
CP310.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the location for the backup application image is securely recorded.	Audit	SR310.
CP311.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that an alert is raised to administrator, if any IoT device or service, is communicating in an abnormal way.	Audit	SR311.
CP312.	IoT device, IoT gateway, Web/Mobile Application	Where possible, ensure that software updates are pushed for a period appropriate to the IoT product. Ensure that this period is made clear to a user when supplying the device. Also, ensure that the supply chain partners inform the user whenever an update is required.	Audit	SR312.
CP313.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the firmware of networking equipment are always be up to date.	Audit	SR313.
CP314.	Cloud/Server	Ensure that the mechanism to manage quick deployment of software updates/patches to servers in production is in place.	Audit	SR314.
CP315.	Cloud/Server	Ensure that the roll-back model is tested for update failures or unexpected issues with production servers.	Audit	SR315.
CP316.	IoT Service Provider	Ensure that the automatic update of configuration is managed.	Audit	SR316.

CP317.	IoT Service Provider	Ensure that a process/plan is in place for validating "updates" and updating IoT components on an on-going basis.	Audit	SR317.
CP318.	IoT device, IoT gateway	For IoT products with no possibility of software update, ensure that the conditions for and period of replacement support is made clear to users during supply of the product.	Audit	SR318.
CP319.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the automatic firmware updates do not modify user-configured preferences, security or privacy settings without permission of the user.	Audit	SR319.
Control-18				
CP320.	IoT Service Provider/ Developer	Ensure that the processes and plans are in place to deal with the security vulnerabilities and exposures.	Audit	SR320.
CP321.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the communication protocols are periodically reviewed and monitored for any publicly known vulnerability and appropriate timely remedial action is taken.	Testing	SR321.
CP322.	IoT Service Provider/Developer	Ensure that the process is in place for consistent briefing of senior executives in the event of the identification of vulnerability or security breach.	Audit	SR322.
CP323.	IoT Service Provider/Developer	Ensure that any statement made in the event of security breach give as full and accurate an account of the facts as possible.	Audit	SR323.
CP324.	IoT Service Provider/Developer	Ensure that a specific contact web page is made available for vulnerability disclosure reporting.	Audit	SR324.
CP325.	IoT Service Provider	Ensure that the dedicated security email address / secure online form for vulnerability communications is made available.	Audit	SR325.

CP326.	IoT Service Provider	Ensure that the vulnerability handling process is compliant with Industry best Practices (e.g. ISO/IEC 30111:2019).	Audit	SR326.
CP327.	IoT Service Provider	Ensure that the mechanism for informing IoT Users and relevant parties regarding vulnerabilities and associated risks are in place.	Audit	SR327.
Control-19				
CP328.	IoT device, IoT gateway, Server, Web/Mobile Application	Ensure that the password entry follows industry standard practice such as recommendations of the 3GPP TS33.117 Password policy or NIST SP800- 63b.	Audit	SR328.
CP329.	IoT device, IoT gateway, Cloud, Server, Web/Mobile Application, Network	Ensure that the product does not accept the usage of weak, null or blank passwords.	Testing	SR329.
CP330.	IoT device, IoT gateway	Ensure that the hardcoded password is not used in IoT components.	Testing	SR330.
CP331.	IoT device, IoT gateway	Ensure that the passwords containing username or common passwords is not allowed.	Testing	SR331.
CP332.	IoT device, IoT gateway	Ensure that IoT components are configured to increase the delay for further attempts, if incorrect password is entered for a predefined number of times.	Testing	SR332.
CP333.	IoT device, IoT gateway, Web/Mobile Application, Server/Cloud, Network	Ensure that the maximum permissible number of consecutive failed user login attempts are as per the password policy.	Testing	SR333.
CP334.	IoT device, IoT gateway	Ensure that the mitigation technique for threshold failed login attempts are implemented on back end side also.	Testing	SR334.
CP335.	IoT Service Provider	Ensure that the factory issued default key/password programmed	Audit	SR335.

		into IoT device or service during manufacturing/provisioning is unique, i.e. no global secret key is shared between multiple devices. – unless this is required by a licensing authority. Also, ensure that the same principle is applied for password-less authentication.		
CP336.	IoT device, IoT gateway	Ensure that the IoT component securely stores passwords using Industry best practices e.g. SP800-63b.	Testing	SR336.
CP337.	IoT device, IoT gateway	Ensure that the password recovery or reset mechanism is secure.	Testing	SR337.
CP338.	IoT device, IoT gateway, Web/Mobile App	Ensure that the product allows an authorised and complete factory reset and all the device's authorisation information.	Testing	SR338.
CP339.	IoT device, IoT gateway	Ensure that the passwords file is owned, accessible and writable by the most privileged account of operating system in case the password is stored in a local file.	Audit	SR339.
CP340.	IoT device, IoT gateway	Ensure that the IoT component is able to detect changes in environmental levels (e.g. voltage, current, operating temperature and humidity etc.) and take appropriate corrective action.	Audit	SR340.
CP341.	IoT device, IoT gateway	Ensure that the IoT component that is used in critical services is enabled with a warning threshold that indicates power-related events such as (Low battery, Black-out, sudden voltage drop, Switch to battery back-up etc.).	Audit	SR341.
CP342.	Mobile Application	Ensure that the configuration is maintained/changed as per IoT security policy.	Audit	SR342.
CP343.	IoT Service Provider/Developer	Where present, ensure that the production software signing keys are under access control.	Audit	SR343.

CP344.	IoT Service Provider/Developer	Ensure that the production software/firmware and identity certificate signing keys are stored and secured in a storage device compliant to FIPS 140-2 level 2, or FIPS 140-3 or ISO/IEC 19790:2012.	Audit	SR344.
CP345.	IoT Service Provider	Ensure that keys are protected against disclosure or copying if facility for key insertion/backup is available in IoT components.	Audit	SR345.
CP346.	IoT Service Provider	Ensure that recovery of IoT components are as per the defined criteria.	Audit	SR346.
CP347.	IoT Service Provider	Ensure that recovery is attempted for a predefined number of attempts.	Audit	SR347.
CP348.	IoT Service Provider	Ensure that IoT component returns to a cryptographically known good state to enable safe recovery and updating of the device.	Audit	SR348.
CP349.	IoT Service Provider	Ensure that the information system resources are periodically changed in the IoT Ecosystem for incorporating additional capacity, application upgradation or implementation of new applications.	Audit	SR349.
CP350.	IoT Service Provider	Ensure that the request for change is initiated by the respective process owners based on Service Call, Request for Service or Incident.	Audit	SR350.
CP351.	IoT Service Provider	Ensure that the preliminary information regarding the change are gathered describing the change, its objectives, benefits, systems needing change and the type of change.	Audit	SR351.
CP352.	IoT Service Provider	Ensure that initial impact and risk analysis is conducted to determine who and what may be affected and the degree of impact.	Audit	SR352.
CP353.	IoT Service Provider	Ensure that the change request is reviewed and approved by the respective team management depending upon the impact	Audit	SR353.

		classification and scope of the change.		
CP354.	IoT Service Provider	Ensure that the change is classified based on who and what will be potentially affected by the change. The implementation procedure and schedule requirements needs to be documented at this stage.	Audit	SR354.
CP355.	IoT Service Provider	Ensure that the post-implementation review is conducted to determine whether the change has achieved the desired goals, assessing the implementation process, validating success, identifying lessons learned and finalizing the change documentation.	Audit	SR355.
CP356.	IoT Service Provider	Ensure that the separate process for emergency changes are in place.	Audit	SR356.
CP357.	IoT Service Provider	Ensure that IoT Ecosystem Service Provider have its security classifications, technical controls in place to manage the classes and to disseminate the data.	Audit	SR357.
CP358.	IoT Service Provider	Ensure that an auditable manifest of all libraries used within the IoT device or service (open source, etc.) to support informed vulnerability management during deployment are maintained.	Audit	SR358.
CP359.	IoT device, IoT gateway	Ensure that the production test and calibration software used during manufacturing of IoT device or service is erased, removed or secured before the IoT device or service is dispatched from the factory or offered for normal usage.	Audit	SR359.
CP360.	IoT device, IoT gateway	Where test and calibration software is required in a service centre, ensure that it is erased or removed upon completion of servicing activity.	Audit	SR360.
CP361.	IoT device, IoT gateway	Where a product includes a trusted Secure Boot process, ensure that the entire production test and any	Audit	SR361.

		related calibration is executed with the processor system operating in its secured boot, authenticated software mode.		
CP362.	IoT Service Provider	Ensure that all physical entities are protected by appropriate controls to ensure that only authorized personnel are allowed to access the respective physical entity.	Audit	SR362.
Control-20				
CP363.	IoT Service Provider/ Developer	Ensure that the IoT Ecosystem Service Provider/Developer provides end users the risks, consequences, and guidance information required for maintenance of privacy and security of IoT Ecosystem.	Audit	SR363.
CP364.	IoT device, IoT gateway, Mobile Application	Ensure that the users are informed about expiry of the IoT product before the end of life.	Audit	SR364.
CP365.	IoT device, IoT gateway	Ensure that the label of IoT device/gateway is accessible to authorized users and contains unique physical identifier and security level.	Testing	SR365.
CP366.	IoT Service Provider/Developer	Ensure that the secure notification process is in place for notifying partners/users about potential risks and required actions related to IoT product.	Audit	SR366.
CP367.	IoT device, IoT gateway	Ensure that the appropriate warning message e.g. “the secure operation may be compromised unless updated” is shown when factory reset of IoT device or service is done.	Testing	SR367.
CP368.	IoT device, IoT gateway	Ensure that the end users are notified whenever remote administration is performed on IoT device or service.	Testing	SR368.
CP369.	IoT Service Provider/Developer	Ensure that the response steps, performance targets and security advisory notification steps are developed for vulnerability disclosures.	Audit	SR369.

CP370.	IoT Service Provider	Ensure that a mechanism is available for notifying connected components of impending downtime for updates, if real time systems are present in IoT ecosystems.	Audit	SR370.
CP371.	IoT Service Provider	Ensure that any update in privacy policy is notified to relevant stakeholders.	Audit	SR371.
CP372.	IoT Service Provider	Ensure that the mechanism for resolving privacy related complaints/feedback and informing relevant stakeholders about any privacy breach is in place.	Audit	SR372.
Control-21				
CP373.	IoT Service Developer	Ensure that the security role (e.g. Development, implementation, testing, integration) of IoT service developer is defined.	Audit	SR373.
CP374.	IoT Service Provider	Ensure that the security role (e.g. Management and Operation) of IoT service provider is defined.	Audit	SR374.
CP375.	IoT Service Provider	Ensure that the security role (e.g. Management and Operation) of IoT user is defined and confirmed during initial set-up procedure.	Audit	SR375.
CP376.	IoT Service Provider	Ensure that the details regarding security roles are communicated to relevant parties.	Audit	SR376.
CP377.	IoT device, IoT gateway	Ensure that the IoT component have stringent access control mechanism for root/highest privilege account to restrict access to sensitive information or system processes.	Testing	SR377.
CP378.	IoT device, IoT gateway	Ensure that the core operating system is segregated from the applications and is only accessible via defined secure interfaces.	Testing	SR378.
CP379.	IoT device, IoT gateway	Ensure that the unprivileged software is restricted from accessing privileged resources.	Testing	SR379.

CP380.	IoT device, IoT gateway	Ensure that the operating system command line access to the most privileged accounts are removed.	Testing	SR380.
CP381.	IoT device, IoT gateway	Ensure that the privileges of applications/services are customized.	Testing	SR381.
CP382.	IoT device, IoT gateway	Ensure that the IoT components only allow controlled user account accesses.	Testing	SR382.
CP383.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the IoT components have provisions to manage and verify multiple cryptographic keys and identities to separate one service/functionality from others.	Testing	SR383.
CP384.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the applications are operated at the lowest privilege level possible and only have access to the resources they need as controlled through appropriate access control mechanisms.	Audit	SR384.
CP385.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the operating system implement a separation architecture to separate trusted execution environment/application from untrusted execution environment/application.	Audit	SR385.
CP386.	IoT Service Provider	Ensure that the components of IoT Ecosystem are securely accessible to administrators for troubleshooting/diagnosing.	Audit	SR386.
CP387.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the changes made by administrators are tracked and visible.	Audit	SR387.
CP388.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that remote administration of IoT components are through secure channel.	Audit	SR388.
CP389.	IoT Service Provider	Ensure that administrators perform the requisite changes after due approvals from respective competent authority.	Audit	SR389.

CP390.	IoT Service Provider	Ensure that IoT Service provider is able to provide proper documents in case partners violate rules related to security classifications.	Audit	SR390.
Control-22				
CP391.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the IoT devices and services are continually monitored to detect the faulty set of functionalities/conditions.	Audit	SR391.
CP392.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the mechanism for alerting end users regarding malicious usage of IoT device or service is in place.	Audit	SR392.
CP393.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the Vulnerability Assessment & Penetration Testing and Application Security Testing are periodically conducted on IoT Ecosystem components in order to detect vulnerable IoT device or service.	Audit	SR393.
Control-23				
CP394.	IoT Service Provider	Ensure that the responsibility is allocated for assessing third party supplied components.	Audit	SR394.
CP395.	IoT Service Provider	Ensure that a point of contact is nominated for third party suppliers with security issues.	Audit	SR395.
CP396.	IoT Service Provider	Ensure that the secure supply chain processes cover the security of development tools and environments, source code repositories, open source dependencies, software update/distribution mechanisms, system images used in factory/provisioning centre.	Audit	SR396.
CP397.	IoT Service Provider	Ensure that a cryptographically protected ownership proof is transferred along the supply chain and extended, if a new owner is added in the chain.	Audit	SR397.
CP398.	IoT Service Provider/ Developer	Ensure that the supplier or manufacturer of any IoT product	Audit	SR398.

		provide information about how the product(s) functions within the end user's network may affect their privacy.		
CP399.	IoT device, IoT gateway, Web/Mobile Application, Network	Ensure that the supplier or manufacturer of IoT component provides clear information about how the IoT component is setup to maintain the end user's privacy and security.	Audit	SR399.
CP400.	IoT Service Provider	Ensure that the supplier or manufacturer of IoT device or service provides user with the information about how IoT component removal or disposal is to be carried out to maintain the end user's privacy and security.	Audit	SR400.
CP401.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the third-party components used in IoT Ecosystem are free from critical vulnerabilities listed in CVE database and the mechanism for periodic checking of it is in place.	Audit	SR401.
Control-24				
CP402.	IoT Service Provider/Developer, IoT User	Ensure that the password policy is in place and follows Industry best practices (e.g. recommendations of 3GPP TS33.117 Password policy, NIST SP800-63b Digital Identity Guidelines – Authentication and Lifecycle Management" or NCSC guidance on password length, characters from the groupings and special characters).	Audit	SR402.
CP403.	IoT device, IoT gateway, Mobile Application	Ensure that an end-of-life policy is published which explicitly states the minimum length of time for which a device will receive software updates and the reasons for the length of the support period. Also, ensure that the need for each update is made clear to users and updates are easy to implement.	Audit	SR403.

CP404.	IoT Application	Ensure that the applicable security features supported by operating system are enabled and used.	Testing	SR404.
CP405.	IoT Application	Ensure that the application follows application security best practices, e.g. OWASP Application Security Verification Standard recommendation.	Testing	SR405.
CP406.	IoT Application	Ensure that the application is free from OWASP Top 10 risks and CWE Top 25 weaknesses.	Testing	SR406.
CP407.	IoT Application	Ensure that the deployment of under-construction/debug/development/test builds of software/firmware in production environment is not allowed.	Testing	SR407.
CP408.	IoT Application	Ensure that the data being transferred over interfaces are validated for the data type, length, format, range, authenticity, origin and frequency.	Testing	SR408.
CP409.	IoT Application	Ensure that the a strong authentication and authorization mechanism is enforced where IoT device or service has a web based user interface.	Testing	SR409.
CP410.	IoT Application	Ensure that the public and restricted areas are separated for authentication where IoT device or service has a web based interface.	Testing	SR410.
CP411.	IoT Application	Ensure that the input in web application is sanitized by performing URL/HTML encoding and treating input as literal text rather than executable script.	Testing	SR411.
CP412.	Web/Mobile Application, API	Ensure that the input and output data is validated using whitelists in line with Industry best practices (e.g. NIST 800-53 Sl-10).	Testing	SR412.
CP413.	Cloud/Server	Ensure that the same security controls are implemented for IPv4 and IPv6 protocols.	Testing	SR413.

CP414.	Cloud/Server	Ensure that the same security controls are implemented for TCP and SCTP protocols, if both are used.	Testing	SR414.
CP415.	Cloud/Server	Ensure that the operating system hardening is done.	Audit	SR415.
CP416.	IoT Application, Cloud/Server	Ensure that all applications deployed in IoT Ecosystem support appropriate cryptographic operations despite technical constraints.	Audit	SR416.
CP417.	IoT Application, Cloud/Server	Ensure that any cryptographic function do not have any publicly known unmitigated weakness and is sufficiently secure for the lifecycle of the device.	Audit	SR417.
CP418.	IoT Application, Cloud/Server	Ensure that the key lengths are sufficient for the level of assurance required as per Industry best practices (e.g. NIST SP800-57).	Audit	SR418.
CP419.	IoT Application/ Gateway, Cloud/Server, Web/Mobile Application, Network	Ensure that the password/pin used by IoT products is not stored or passed over the network in plaintext, even if the communication channel is secured through encryption.	Audit	SR419.
Control-25				
CP420.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the contact details for support services related to IoT device or service is made available to end users.	Audit	SR420.
Control-26				
CP421.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the factory set properties for initial use of IoT Ecosystem components is appropriate and their importance are identified and documented.	Testing	SR421.
CP422.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the product supports having any or all the factory default user login passwords altered when installed or commissioned.	Audit	SR422.
CP423.	IoT device, IoT gateway, cloud,	Where a user interface password is used for login authentication,	Audit	SR423.

	Web/Mobile Application	ensure that the factory issued or reset password is unique to each device in the product family. If a password-less authentication is used, ensure that the same principles of uniqueness apply.		
CP424.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that IoT components with inbuilt WiFi access points for initial setup is adequately protected.	Audit	SR424.
CP425.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that a robust authentication requiring physical interaction with the component or possession of a one-time token (e.g. pre-shared key, QR Code) is used for initial pairing with the device.	Testing	SR425.
CP426.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the new settings are not same as the original, are not shared with other IoT device or service setting, are not easily guessable and are not available on the list of popular ID/password list available on the Internet.	Audit	SR426.
Control-27				
CP427.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the IoT device is turned off when it is no longer or not in used.	Testing	SR427.
Control-28				
CP428.	IoT device, IoT gateway	Ensure that a secure revocation and decommissioning procedure is defined for secure disposal on end of life of IoT device.	Audit	SR428.
CP429.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that any sensitive data and licensed software is removed or securely overwritten prior to disposal or re-use.	Audit	SR429.
CP430.	IoT device, IoT gateway, cloud, Web/Mobile Application	Where an IoT device or service can have their ownership transferred to a different owner, ensure that the previous owner's entire personal information is securely removed from the IoT device or service.	Audit	SR430.

		Ensure that this option is available when a transfer of ownership occurs or when an end user wishes to delete their personal information from the IoT device or service.		
CP431.	IoT device, IoT gateway, cloud, Web/Mobile Application	Where a device or service user wishes to end the service, ensure that all Personal Information of the user is removed from the device and related services.	Audit	SR431.
CP432.	IoT device, IoT gateway, cloud, Web/Mobile Application	Where a device or service user wishes to end the service, ensure that all linkages of the user to the device identity are removed.	Audit	SR432.
CP433.	IoT device, IoT gateway, Web/Mobile Application	In case of ownership change, ensure that the device or service have an irrevocable method of decommissioning and recommissioning.	Audit	SR433.
CP434.	IoT device, IoT gateway, Web/Mobile Application	Ensure that the IoT device or service registration with IoT Service Provider is secure.	Audit	SR434.
CP435.	IoT device, IoT gateway, Web/Mobile Application	Ensure that the device manufacturer makes sure that the identity of the device is independent of the user, to ensure anonymity.	Audit	SR435.
Control-29				
CP436.	IoT Service Provider	Ensure that IoT Service Provider defines what types of information are acquired, generated and disseminated to peers in IoT Ecosystem, and how these types of data are treated.	Audit	SR436.
CP437.	IoT Service Provider	Ensure that the type identifies what the data represents and how it needs to be processed.	Audit	SR437.
CP438.	IoT Service Provider	Ensure that the security classification of data are done to represent how, where, and when the information can be used and to whom it may be shared.	Audit	SR438.

CP439.	IoT Service Provider	Ensure that the awareness/training programs specific to IoT security/privacy are periodically conducted for personnel handling data processing.	Audit	SR439.
CP440.	IoT Service Provider	Ensure that IoT Ecosystem uses anonymous attestation techniques for proving of identity and maintaining privacy (e.g. As per Open ID mechanism, Enhanced Privacy ID 2.0, DAA or ISO/IEC 20008: 2013 or ISO/IEC 20009: 2017).	Audit	SR440.
CP441.	IoT Service Provider	Ensure that the data is erased from all IoT components including companion Mobile application/Backend servers on receiving request for erasure from user.	Audit	SR441.
CP442.	IoT Service Provider	Ensure that IoT Ecosystem is compliant with relevant data protection and data localization laws of India.	Audit	SR442.
CP443.	IoT device, IoT gateway, Web/Mobile Application	Ensure that protocol anonymity features are enabled in protocols (e.g. Bluetooth) to limit location tracking capabilities.	Audit	SR443.
Control-30-1				
CP444.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the PII is protected by default settings built into the IoT products without the need of any user intervention.	Audit	SR444.
CP445.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the proper access control is implemented in the IoT product.	Audit	SR445.
CP446.	IoT device, IoT gateway, cloud/Server, Web/Mobile Application, Network	Ensure that all personal information are encrypted both in transit and at rest.	Audit	SR446.

CP447.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the provision for restoration to a "default" secure and privacy state is available.	Testing	SR447.
Control-30-2				
CP448.	IoT Service Provider	Ensure that the strictest privacy settings are applied by default, without any intervention of IoT user.	Audit	SR448.
CP449.	IoT device, IoT gateway, Web/Mobile Application	Ensure that the user decision points that may have a detrimental impact on security and privacy are minimized.	Audit	SR449.
Control-31-1				
CP450.	IoT Service Provider	Ensure that IoT Ecosystem stores the minimum amount of personal information from users required for the operation of the service.	Audit	SR450.
CP451.	IoT Service Provider	Ensure that IoT Ecosystem Service provider have defined privacy policy, processes and procedure.	Audit	SR451.
CP452.	IoT Service Provider	Ensure that the categories of users whose data are being processed is maintained.	Audit	SR452.
CP453.	IoT Service Provider	Ensure that the categorization of data with their sensitivity levels is maintained.	Audit	SR453.
CP454.	IoT Service Provider	Ensure that the purpose and elements of data actions, identification of potential problematic data actions, associated privacy risk tolerances, actions pending is identified and periodically reviewed.	Audit	SR454.
CP455.	IoT Service Provider	Ensure that the obtained/communicated data from/to IoT devices and systems and their importance are identified and documented.	Audit	SR455.
Control-31-2				
CP456.	IoT Service Provider	Ensure that users are provided a checklist of the collected personal information, its purpose, time limit and intended usage of their data.	Testing	SR456.

CP457.	IoT Service Provider	Ensure that only consent based collection and retention of personal information is permitted, and the collected information is destroyed after the consented use or duration.	Audit	SR457.
Control-32				
CP458.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the independent verification of IoT device, data components and IoT service components is conducted before first putting IoT Ecosystem for public use.	Audit	SR458.
CP459.	IoT Service Provider	Ensure that the revocation of capabilities take place on immediate basis.	Audit	SR459.
CP460.	IoT Service Provider	Ensure that the rights of users are evaluated periodically.	Audit	SR460.
Control-33				
CP461.	IoT device, IoT gateway, Web/Mobile Application	Ensure that the authorised users are able to securely change the configuration.	Testing	SR461.
CP462.	IoT device, IoT gateway, Web/Mobile Application	Ensure that the security features of IoT devices and services are user-friendly.	Audit	SR462.
CP463.	IoT device, IoT gateway, Web/Mobile Application	Ensure that the implicit/explicit requirements and concerns of users are addressed in design.	Audit	SR463.
Control-34				
CP464.	IoT device, IoT gateway, cloud, Web/Mobile Application	Ensure that the implementation of security, privacy and trustworthiness features in IoT device or service are accompanied with threat modelling and risk assessment.	Audit	SR464.
CP465.	IoT Service Provider	Ensure that the effectiveness of privacy controls is reviewed periodically and new risks are identified. Also, ensure that the privacy impact assessment is conducted on continually considering needs of end users and regulatory requirements. This	Audit	SR465.

		should extend to data gathered beneath Web APIs from third party platform suppliers.		
Control-35-1				
CP466.	IoT device, IoT gateway	Ensure that unique logical and physical identifier is assigned to each IoT device/gateway/component.	Testing	SR466.
CP467.	IoT device, IoT gateway, Web/Mobile Application	Ensure that the statistically unique identity is provisioned binding code and data to specific instance.	Testing	SR467.
CP468.	IoT device, IoT gateway, Web/Mobile Application	Ensure that the unique identity is used for maintaining the status of instance.	Testing	SR468.
CP469.	IoT device, IoT gateway, Web/Mobile Application	Ensure that the backup of identity is kept in tamper resistant back-end systems.	Audit	SR469.
CP470.	IoT device, IoT gateway, Web/Mobile Application	Ensure that the provisioning happens in field and involves unique mapping between IoT device and IoT user.	Audit	SR470.
CP471.	IoT device, IoT gateway, Web/Mobile Application	Ensure that the identity used for establishing communications link to each IoT service is securely provisioned, stored and managed.	Testing	SR471.
CP472.	IoT device, IoT gateway	Ensure that the secure trust anchor performs all cryptographic operations (e.g. key generation, signing, signature verification, symmetric & asymmetric encryption).	Audit	SR472.
CP473.	IoT device, IoT gateway, Web/Mobile Application	Ensure that the unique identity key is generated and stored in secure trust anchor. In case key storage is done outside, ensure that the storage is encrypted with instance specific secret key residing in secure trust anchor.	Audit	SR473.

CP474.	IoT Service Provider	Ensure that trust delegation is implemented for root of trust keys.	Audit	SR474.
CP475.	IoT device, IoT gateway, Web/Mobile Application	Ensure that the root signing key is issued by Certifying Authorities recognised by CCA.	Testing	SR475.
CP476.	IoT Service Provider	Ensure that the root key is securely generated and used for signing keys of each sub-organization or third party in hierarchy of IoT Ecosystem.	Audit	SR476.
CP477.	IoT Service Provider	Ensure that the sub-organizations securely generate their other keys and use the key signed with root key to sign the subsequently generated keys (e.g. Code signing Key, Server Communication Key, Peer-to-Peer Communication Key, IoT Device Identity Key) which are used in sub-ordinate IoT Ecosystem hierarchy.	Audit	SR477.
CP478.	IoT Service Provider	Ensure that the trust delegation have provisions for centralized or decentralized root of trust, identity provisioning and revocation.	Audit	SR478.
CP479.	IoT Service Provider	Ensure that the trust delegation mechanism ensures that each entity in IoT Ecosystem is authorized by the same organization as any peer.	Audit	SR479.
CP480.	IoT Service Provider	Ensure that a central organization acts as the owner of IoT Ecosystem chain of trust.	Audit	SR480.
CP481.	IoT Service Provider	Ensure that any compromised key/certificate is revoked at the earliest by authorized personnel.	Audit	SR481.
CP482.	IoT device, IoT gateway, Web/Mobile Application	Ensure that the trust chain of identity certificate is traceable to root signing key of the organization.	Testing	SR482.
CP483.	IoT device, IoT gateway, Web/Mobile Application	Ensure that the identity is verified by authorized services through remote attestation mechanisms	Testing	SR483.

		(e.g. Challenge Response Mechanism).		
CP484.	IoT device, IoT gateway, Web/Mobile Application	Ensure that the remote attestation is used in mutual authentication of IoT device/gateway and backend server before allowing access of resources.	Testing	SR484.
CP485.	IoT device, IoT gateway, Web/Mobile Application	Ensure that the identity certificates whose trust chain is traceable to root signing key is only allowed access/operation in IoT Ecosystem of the user organisation.	Testing	SR485.
CP486.	IoT device, IoT gateway, Web/Mobile Application	Ensure that the root of trust/identity is available within the device to authenticate network components/communications and authenticate itself to network peers.	Audit	SR486.
CP487.	IoT device, IoT gateway, Web/Mobile Application	Ensure that any updatable digital certificate is updated only through secure means.	Audit	SR487.
CP488.	IoT Service Provider	Ensure that the public identity certificate is maintained in the back-end servers and is available on request.	Audit	SR488.
CP489.	IoT device, IoT gateway	Ensure that the integrity of IoT component application platform is verified with the help of identity and secure trust anchor prior to execution of firmware/software of IoT component.	Audit	SR489.
CP490.	IoT device, IoT gateway	Ensure that the security-centric data is processed within secure RAM that is internal to CPU or secure trust anchor.	Audit	SR490.
CP491.	IoT device, IoT gateway	Ensure that the TEE and other applications on the IoT component do not interact with a peer if trust anchor cannot validate the peer after pre-defined re-attempts.	Audit	SR491.
Control-35-2				
CP492.	IoT Service Provider	Ensure that the data store on server is mapped to access rights, time	Testing	SR492.

		duration and unique identity of IoT device/service, partner or user.		
CP493.	IoT Service Provider	Ensure that the devices that may be used by more than one individual have mechanism to uniquely attribute the device to an user on receipt of authorised request.	Audit	SR493.
CP494.	IoT Service Provider	Ensure that the devices or services that may be used by more than one individual have mechanism to enforce user preferences of the last authenticated user of IoT Device or Service. In case user is logged out, the device or service should enforce user preferences only after authentication process is complete.	Audit	SR494.
Control-36				
CP495.	IoT device, IoT gateway, Web/Mobile Application, API	Ensure that an independent mechanism is available to confirm that the right device was accessed and action was completed.	Audit	SR495.
CP496.	IoT device, IoT gateway, Web/Mobile Application, API	Ensure that implemented authentication cannot be bypassed, tampered or falsified in any known reasonable method.	Audit	SR496.
Control-37				
CP497.	IoT device, IoT gateway	Ensure that the IoT component uses random radio address for connecting to new environments.	Testing	SR497.
CP498.	IoT device, IoT gateway	Where RF communications are enabled (e.g., ZigBee, etc.), ensure that the antenna power are configured to limit ability of mapping assets to limit attacks such as WAR-Driving.	Testing	SR498.
CP499.	IoT Service Provider	Ensure that unauthorized collection and analysis of metadata by third parties is strictly controlled.	Audit	SR499.
CP500.	IoT Service Provider	Ensure that the collected indirect data (e.g. IP address, Geo Location, Contextual information, nearby devices' information, temperature etc.) is bare minimum required for functioning of IoT Ecosystem, unless explicitly consented by user.	Audit	SR500.
Control-38				

CP501.	IoT device, IoT gateway, Web/Mobile Application	Ensure that only authenticated and authorised users are allowed to add, modify or delete user preferences of privacy controls.	Audit	SR501.
Control-39				
CP502.	IoT Service Provider	Ensure that a secondary independent verification is a prerequisite to any automated decision making that leads to an irreversible harm.	Audit	SR502.
Control-40				
CP503.	IoT Service Provider	Ensure that the list of systems/products/services/devices handling data processing are maintained along with environment (e.g. geographical location i.e. internal, cloud, third party) and processing location identifier for visibility.	Audit	SR503.
CP504.	IoT Service Provider	Ensure that the roles and responsibilities of stakeholders handling data processing is in place.	Audit	SR504.
Control-41				
CP505.	IoT Service Provider	Ensure that IoT device unique identifier allows traceability, analytics and fraud management, if applicable.	Audit	SR505.
CP506.	Cloud, IoT Service Provider	Ensure that IoT Service Provider does not have the ability to do a reverse lookup of device ownership from the device identity.	Audit	SR506.
CP507.	IoT Service Provider	Ensure that the disassociated/anonymized processing of data is done in unobservable/ unlinkable manner in case of any reporting required.	Audit	SR507.
CP508.	IoT device, IoT gateway	Ensure that unique binary identifiers used for communication modules are not collected until necessary.	Audit	SR508.
CP509.	IoT device, IoT gateway, Web/Mobile Application, API	Ensure that external users are not able to use APIs of IoT Ecosystem for deriving hardware serial numbers or other trackable identities from user profiles.	Audit	SR509.
Control-42				
CP510.	IoT device, IoT gateway,	Ensure that the actions, activities or behaviours are not exposed to third parties.	Audit	SR510.

	Web/Mobile Application, API			
CP511.	IoT Service Provider	Ensure that any data shared with third party contains data processing permissions in metadata.	Audit	SR511.
CP512.	IoT Service Provider	Ensure that the accountability matrix defining entity responsible for any potential data breach is available.	Audit	SR512.
CP513.	IoT Service Provider	Ensure that the entity responsible for responding to any data breach or data disclosure request is defined.	Audit	SR513.
Control-43				
CP514.	IoT Service Provider	Ensure that the web/mobile application with granular consent management capabilities is made available to users.	Audit	SR514.
CP515.	Web/Mobile Application	Ensure that the web/mobile application allows users to easily grant or revoke consent for use of personal data by IoT device or service.	Audit	SR515.
CP516.	Web/Mobile Application	Ensure that the application allows users to withdraw consent in case IoT output is no longer need or there is concern with the IoT device or service.	Audit	SR516.
CP517.	Web/Mobile Application	Ensure that the web/mobile application allows users to set auto-delete timeframe for collected PII data.	Audit	SR517.
CP518.	Web/Mobile Application	Ensure that users have validation mechanism available with respect to default settings built into the IoT device or service.	Audit	SR518.
CP519.	Web/Mobile Application	Ensure that the IoT device or service records audio, visual, geospatial or health data only after obtaining explicit consent of the user.	Audit	SR519.
CP520.	Web/Mobile Application	Ensure that the users of IoT ecosystem are able to exercise their rights to information access, erasure, rectification, data portability, restriction of processing and objection to processing.	Audit	SR520.

CP521.	Web/Mobile Application	Ensure that the consent is obtained where IoT user's metrics is used for optimization of the usage of IoT Ecosystem.	Audit	SR521.
Control-44				
CP522.	IoT device	Ensure that IoT device connects with other device or service only if there is a valid need.	Audit	SR522.
CP523.	IoT device, IoT gateway	Ensure that mechanism for detecting and alerting is in place whenever a device or service is requested without valid need.	Audit	SR523.
Control-45				
CP524.	IoT device, IoT gateway, Cloud, Network, Web/Mobile Application	Ensure that the certification/validation of privacy preserving features are conducted for IoT devices or services used in the IoT Ecosystem.	Audit	SR524.
CP525.	IoT device, IoT gateway, Cloud, Network, Web/Mobile Application	Ensure that IoT users are provided information regarding certification/validation conducted on IoT device or service.	Audit	SR525.

Bibliography

[1] IoT Security Assurance Framework, Release 3.0, IoT Security Foundation, November 2021.
[2] OWASP Application Security Verification Standard - Version 3.0.1.
[3] OWASP Mobile Application Security Verification Standard - Version 1.1.
[4] Internet of Things Reference Architecture, ISO/IEC 30141.
[5] Solutions to Enhance IoT Authentication Using SIM Cards (UICC), November 30, 2016, GSMA
[6] IoT Security Guidelines, October 2017, GSMA
[7] Hardware IoT Security White Paper, Version 2.0, 2017, Huawei.
[8] IoT Security Whitepaper, PubNub
[9] Baseline Security Recommendation for IoT, November 2017, ENISA
[10] NIST 8259 - Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers
[11] NISTIR 8228 - Core Cybersecurity Feature Baseline for Securable IoT Devices
[12] IoT Reference Framework, November 2018, IoT ALLIANCE AUSTRALIA
[13] Benchmark for Internet of Things, Center for Internet Security
[14] OCF Security Specification, Ver. 2.0.4, July 2019
[15] NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management Dated September 6, 2019
[16] NISTIR 8267: Security Review of Consumer Home IoT Products
[17] NIST SP 800-207: Zero Trust Architecture
[18] CWE Top 25 2020
[19] IoT Policy Document, MeitY Government of India.