Doc No: LITD 17(19143)

इंटरनेट ऑफ थिंग्स सुरक्षा और गोपनीयता : आकलन और मूल्यांकन

Internet of Things Security & Privacy
: Assessment and Evaluation

Or

Implementation Guidance for IoT Device Security and Privacy

ICS 35.030

BUREAU OF INDIAN STANDARDS

MANAKBHAVAN, 9 BAHADURSHAHZAFAR MARG

NEW DELHI 110002

May 2024 **Price Group**

Information System Security and Privacy Sectional Committee, LITD 17
(Formal Clauses to be added later on)

FOREWORD

This Indian Standard may be adopted by the Bureau of Indian Standards, after the draft finalized by Information System Security and Privacy Sectional Committee may be approved by the Electronics and Information Technology Divisional Council.

This document is tailored for a diverse audience, including:

- IoT device manufacturers, seeking to enhance the security and privacy features of their products.
- System integrators and solution architects, tasked with creating secure IoT ecosystems.
- IT and security professionals responsible for safeguarding IoT deployments.
- Regulators and compliance officers overseeing adherence to IoT security and privacy standards.

Introduction

IoT has rapidly evolved, embedding itself in our daily lives and various industries, presenting a pressing need to safeguard the confidentiality, integrity, and privacy of data collected and transmitted by these devices. The proliferation of IoT devices has ushered in a new era of convenience and efficiency, yet this progress is accompanied by a growing concern for security and privacy. As more devices connect to the internet, they become potential targets for cyberattacks, data breaches, and privacy violations.

This document aims to address these challenges by offering guidance on securing IoT devices and preserving user privacy, thereby ensuring the continued growth and trustworthiness of the IoT landscape.

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.

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

This document provides comprehensive guidance on establishing robust security and privacy measures for IoT (Internet of Things) devices.

This guidance specifically addresses the critical aspects of IoT device security and privacy. It aims to equip IoT device manufacturers, system integrators, and other stakeholders with the knowledge and tools required to:

- Design and produce IoT devices with robust security features that mitigate vulnerabilities and resist unauthorized access.
- Implement privacy-preserving mechanisms that ensure the responsible handling of sensitive user data.
- Adhere to established IoT security and privacy standards and regulations.
- Foster a culture of continuous improvement to adapt to emerging threats and evolving technologies.

Contents

1. Scope

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

2. Normative References

The standards given below contains provisions, which through reference in this text constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreement based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed as follows:

IS/ISO/IEC 27400:2022 - Cybersecurity — IoT security and privacy — Guidelines.

IS/ISO/IEC 27402:2023 Cybersecurity — IoT security and privacy — Device baseline requirements

Open Web Application Security Project (OWASP). Version 4.0.3. ASVS Appendix C - IoT Security.

3. Acronyms

4. Terms and Definitions

For the purpose of this document, the terms and definitions given in IS/ISO/IEC 27000, IS/ISO/IEC 27400 apply.

5. Risk Assessment and Threat Modelling

5.1 Conducting a Risk Assessment for IoT Systems

In the context of IoT device security and privacy standards, it is mandated that IoT devices undergo a comprehensive risk assessment process at the device level, which is an integral part of a broader system-level risk assessment. This assessment must encompass several key considerations:

1. Intended Outcomes: The risk assessment process must take into account the intended outcomes specific to the intended use case of the IoT device.
2. Stakeholder Needs and Expectations: The risk assessment process should also consider the needs and expectations of all relevant stakeholders, including those who are part of networks to which the IoT device connects. This assessment should address both physical and logical undesired effects.
3. Device Constraints: Recognizing that IoT devices often operate under constraints such as limited battery life, minimal memory, or constrained processing capabilities, these limitations should inform the risk treatment process.

The following guidelines and processes must be adhered to:

- **Product Differentiation:** Determine if separate risk assessment and treatment processes are warranted for different IoT products.

- **Risk Treatment Options:** Select appropriate risk treatment options based on the outcomes of the risk assessment.
- **Control Implementation:** Identify all necessary controls required to implement the chosen risk treatment options.
- **Security and Privacy Features Identification:** Identify all security and privacy features associated with the IoT device that stem from the identified control.
- **Feature Verification:** Compare the identified features to ensure that none are omitted inadvertently.
- **Statement of Applicability:** Create a Statement of Applicability that includes the essential features and provides justifications for their inclusion or exclusion.
- **Adherence to Other Standards:** If other standards related to device requirements are applicable, ensure compliance with the requirements of those standards.
- **Risk Treatment Plan:** Develop a comprehensive risk treatment plan that outlines the steps and actions to mitigate identified risks.
- **Risk Owner Communication:** Communicate the risk treatment plan to the designated risk owner, along with any residual risks. Obtain the risk owner's approval of the plan and their acknowledgment of any remaining risks, where applicable.

Furthermore, IoT devices must implement the identified necessary features and controls outlined in the Statement of Applicability. This implementation must extend to all requisite features and controls.
Documentation for the entire risk assessment process, security and privacy features, omitted requirements, vulnerability disclosure processes, and security support policy must remain available and accessible throughout the supported lifetime of IoT devices.

5.2 Identifying Potential Risks

IoT device security and privacy are vulnerable to a range of threats and vulnerabilities. Understanding these risks is crucial for effective risk management. Below are some risks in the IoT landscape:

Sl. No.	Risk
R1	Failure to define, approve, and communicate an IoT security policy may result in inadequate measures to mitigate security threats, leaving devices vulnerable to exploitation.
R2	Undefined roles and responsibilities for IoT security may lead to ambiguity in accountability, potentially resulting in overlooked security measures and increased susceptibility to breaches.
R3	Incomplete identification of assets during IoT device development may overlook critical components, leading to inadequate protection of sensitive data and assets.
R4	Absence of mechanisms to apply insights from past security incidents may perpetuate vulnerabilities, increasing the likelihood and impact of future breaches.
R5	Unprotected application layer debugging interfaces pose a risk of unauthorized access and exploitation, compromising the integrity and confidentiality of the device.

R6	Failure to enable memory protection controls exposes the IoT device to memory-based attacks, jeopardizing the confidentiality and integrity of stored data.
R7	Active on-chip debugging interfaces pose a threat of unauthorized access and manipulation, potentially leading to exploitation and compromise of device functionality.
R8	Lack of implementation of trusted execution may allow unauthorized access to critical functions and data, compromising the confidentiality and integrity of the device.
R9	Insecure storage of sensitive data and cryptographic assets increases the risk of unauthorized access and compromise, potentially leading to data breaches and exploitation.
R10	Inadequate random number generation may lead to predictable cryptographic keys and compromise the confidentiality and integrity of communication channels.
R11	Exposure of sensitive traces on the printed circuit board increases the risk of physical tampering and unauthorized access, potentially compromising device security.
R12	Unencrypted inter-chip communication exposes sensitive data to interception and manipulation, increasing the risk of data breaches and unauthorized access.
R13	Lack of code signing and validation exposes the device to the risk of executing malicious or tampered firmware, compromising device integrity and functionality.
R14	Failure to overwrite sensitive data in memory increases the risk of data leakage and unauthorized access, potentially leading to exposure of sensitive information.
R15	Inadequate isolation between firmware apps may facilitate unauthorized access and compromise of sensitive data and device functionality.
R16	Failure to configure secure compiler flags exposes firmware to various exploitation techniques, compromising device security and integrity.
R17	Lack of code protection in microcontrollers increases the risk of unauthorized access and manipulation of firmware, compromising device functionality and security.
R18	Use of banned C functions poses a risk of vulnerabilities and exploitation, potentially compromising device security and integrity.
R19	Incomplete documentation of third-party components and vulnerabilities increases the risk of exploitation and compromise through known vulnerabilities.
R20	Failure to review code for hardcoded credentials exposes devices to unauthorized access and exploitation, compromising device security.
R21	Inactive Intellectual Property protection technologies may lead to unauthorized reproduction and exploitation of device functionality, compromising intellectual property rights.
R22	Lack of support for disabling debugging interfaces in microcontrollers increases the risk of unauthorized access and manipulation, compromising device security.
R23	Inadequate protection from physical attacks increases the risk of reverse engineering and exploitation, compromising device security and confidentiality.

R24	Insufficient integration of security measures may result in vulnerabilities that could lead to malfunction or compromise of the device, posing safety risks.
R25	Failure to protect data-in-transit exposes sensitive information to interception and manipulation, compromising data confidentiality and integrity.
R26	Lack of validation of server connections exposes the device to the risk of connecting to malicious servers, compromising data confidentiality and integrity.
R27	Failure to mutually authenticate wireless communications increases the risk of unauthorized access and interception, compromising data confidentiality and integrity.
R28	Unencrypted wireless communications expose sensitive information to interception and manipulation, compromising data confidentiality and integrity.
R29	Failure to pin digital signatures to trusted servers exposes devices to the risk of connecting to malicious servers, compromising data confidentiality and integrity.
R30	Inadequate monitoring and logging of device states, events, and network traffic hinder detection and response to security incidents, increasing the risk of exploitation and compromise.
R31	Insecure storage of logs increases the risk of unauthorized access and manipulation, potentially compromising the integrity and confidentiality of logged information.
R32	Absence of tamper resistance and detection features increases the risk of physical tampering and unauthorized access, compromising device security.
R33	Delivery of IoT devices with insecure settings and configurations increases the risk of exploitation and compromise, jeopardizing device security.
R34	Unauthorized modification of IoT device configurations poses a risk of exploitation and compromise, compromising device security and functionality.
R35	Use of common values for critical security parameters increases the risk of exploitation and compromise, compromising device security and confidentiality.
R36	Absence of security controls against firmware reverse engineering increases the risk of unauthorized access and manipulation, compromising device security and integrity.
R37	Failure to implement authentication mechanisms increases the risk of unauthorized access to IoT systems and services, compromising data confidentiality and integrity.
R38	Inadequate protection of stored and transmitted data increases the risk of unauthorized access and manipulation, compromising data confidentiality and integrity.
R39	Vulnerability to OS Command Injection poses a risk of unauthorized access and manipulation, compromising device security and integrity.
R40	The absence of defined update procedures heightens the risk of unauthorized updates and exploitation.
R41	Unauthorized initiation of software updates for IoT devices can lead to exploitation of vulnerabilities or implantation of malicious code.
R42	Vulnerability to time-of-check vs time-of-use attacks during updates increases the risk of installing malicious or tampered firmware, compromising device integrity.
R43	Failure to validate firmware upgrade files before installation poses a security risk by potentially allowing the installation of malicious or tampered firmware,

	while neglecting verification of the cryptographic chain of trust during updates exacerbates this risk, jeopardizing device integrity and potentially compromising user privacy.
R44	Ability to downgrade to old firmware versions increases the risk of exploiting known vulnerabilities, compromising device security and functionality.
R45	Inadequate monitoring and reporting of vulnerabilities increases the risk of exploitation and compromise, jeopardizing IoT device as well as user security.
R46	Failure to wipe firmware and sensitive data upon tampering or receipt of invalid messages increases the risk of unauthorized access and manipulation, compromising device security.
R47	Lack of guidance on proper IoT device usage increases the risk of misuse and exploitation, compromising device security and functionality.
R48	Inadequate evaluation of supplier security measures increases the risk of acquiring insecure IoT device components, jeopardizing overall IoT device security.
R49	Unauthorized disclosure of IoT device security information increases the risk of exploitation and compromise, jeopardizing device security and confidentiality.
R50	Inadequate removal of data and licensed software prior to disposal or re-use increases the risk of unauthorized access and exposure of sensitive information, compromising data confidentiality and integrity.
R51	Absence of a secure function to delete user data increases the risk of unauthorized access and exposure of sensitive information, compromising data confidentiality and integrity.
R52	Failure to incorporate privacy-enhancing features increases the risk of privacy violations and unauthorized access to personal data, compromising user privacy.
R53	Failure to ensure the strictest privacy settings by default increases the risk of privacy violations and unauthorized access to personal data, compromising user privacy.
R54	Lack of privacy notice detailing the data collection purpose increases the risk of unauthorized data collection and misuse, compromising user privacy.
R55	Failure to obtain consent before data collection increases the risk of unauthorized data collection and misuse, compromising user privacy.
R56	Failure to address end users' privacy concerns in device design increases the risk of privacy violations and unauthorized access to personal data, compromising user privacy.
R57	Lack of regular review of privacy controls increases the risk of privacy violations and unauthorized access to personal data, compromising user privacy.
R58	Failure to assign unique cryptographic keys and certificates increases the risk of unauthorized access and impersonation, compromising device privacy and security.
R59	Inadequate mapping of device identifiers to specific individuals increases the risk of privacy violations and unauthorized access to personal data, compromising user privacy.
R60	Failure to enforce authorized access increases the risk of unauthorized access and manipulation
R61	Unauthorized data collection risks compromising user privacy and autonomy.
R62	Insufficient authentication may lead to unauthorized privacy preference manipulation.
R63	Lack of secondary verification could result in irreversible harm to IoT users.

R64	Absence of an accountability framework increases the likelihood of data mishandling and privacy breaches, diminishing transparency and accountability in data processing practices.
R65	Poorly managed PII protection increases the risk of unauthorized access and disclosure.

5.3 Prioritizing Security and Privacy Risks

After identifying potential risks, it's essential to prioritize them based on their impact and likelihood. This prioritization informs resource allocation and risk mitigation efforts.

Factors to Consider in Prioritizing Risks:

1. Impact: Assess the potential consequences of a security or privacy breach. Consider the financial, operational, reputational, and legal ramifications.

2. Likelihood: Estimate the likelihood of each risk occurring. Consider historical data, industry trends, and specific contextual factors.

3. Risk Tolerance: Define the organization's risk tolerance level. Some risks may be accepted if they fall within acceptable limits, while others require immediate mitigation.

4. Dependencies: Recognize interdependencies among risks. Addressing one risk may mitigate or exacerbate others.

5. Regulatory Compliance: Prioritize risks that have implications for regulatory compliance, as non-compliance can result in legal penalties.

By conducting a thorough risk assessment and prioritizing security and privacy risks, organizations can develop a targeted strategy for implementing security controls and privacy safeguards. This approach ensures that resources are allocated effectively to protect IoT devices against the most significant risks.

6. IoT Device Security Checklist

IoT device security is a critical component of ensuring the overall security and privacy of an IoT system. Devices are the frontline defense against potential threats and vulnerabilities. This section provides guidance on key aspects of IoT device security and privacy, helping organizations mitigate risks associated with IoT devices.

To ensure a comprehensive approach to security and privacy, organizations often categorize their security measures into different levels, with each level representing a different degree of security rigor and complexity. Here's an overview of the three levels:

Level 1: Basic Security and Privacy

At Level 1, the focus is on implementing fundamental security and privacy measures to provide a baseline level of protection for IoT devices and data. This level is suitable for simple IoT deployments and devices with limited capabilities.

Level 2: Enhanced Security and Privacy
Level 2 involves a more robust security and privacy approach, suitable for more complex IoT deployments and devices that handle sensitive data or operate in more challenging environments.

Level 3: Advanced Security and Privacy
Level 3 represents the highest level of security and privacy for IoT devices and systems. It is suitable for mission-critical applications, highly sensitive data, and deployments in high-risk environments.

The choice of security and privacy level depends on factors such as the IoT device's purpose, the data it handles, the potential impact of security breaches, and the regulatory environment. Organizations should conduct a thorough risk assessment to determine the appropriate level of security and privacy controls needed for their specific IoT deployments.

Additionally, compliance with relevant industry standards and regulations, such as IT Act, Digital Data Protection Act, should also be considered when defining security and privacy requirements for IoT devices.

Sl. No.	Security & Privacy Checkpoint	L1	L2	L3	Associated Risk
1. Security Controls					
1.1 Security controls for IoT service developer and IoT service provider					
1.1.1 Policy for IoT security					
Control-1: A policy for IoT security should be defined, approved by management, published, communicated to relevant personnel and relevant external parties and reviewed at planned intervals or if significant changes occur.					
V1.1	Ensure that a policy for IoT security is defined, approved by management, published, communicated to relevant personnel and relevant external parties and reviewed at planned intervals or if significant changes occur.			✓	R1
1.1.2 Organization of IoT security					
Control-2: Roles and responsibilities for security of IoT should be defined and allocated.					
V2.1	Ensure that the roles and responsibilities for security of IoT device is defined and allocated.			✓	R2
1.1.3 Asset management					
Control-3: Information, IoT devices and systems and their functions and operations to be protected should be identified.					
V3.1	Confirm that the IoT device developer has identified all assets (Information, IoT devices and systems) to be protected across the entire development process of the IoT device.			✓	R3
1.1.4 Equipment and assets located outside physical secured areas					
Control-4: Specific security measures should be applied to IoT equipment and assets which are located or operated outside physical secured areas.					

Not Applicable for IoT Device Assessment (Applicable for IoT Ecosystem)					
1.1.5 Secure disposal or re-use of equipment					
Control-5: All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.					
Not Applicable for IoT Device Assessment (Applicable for IoT Ecosystem)					
1.1.6 Learning from security incidents					
Control-6: Knowledge gained from analysing and resolving IoT security incidents should be used to reduce the likelihood or impact of future incidents.					
V6.1	Ensure that mechanisms are in place to apply knowledge gained from analyzing and resolving IoT device security incidents to reduce the likelihood or impact of future incidents.			✓	R4
1.1.7 Secure IoT system engineering principles					
Control-7: Principles for engineering secure IoT systems that address designing and implementation of security functions, defence in depth and hardening of systems and software should be applied to the development of IoT systems.					
V7.1	Verify that application layer debugging interfaces such USB, UART, and other serial variants are disabled or protected by a complex password.	✓	✓	✓	R5
V7.2	Verify that memory protection controls such as ASLR and DEP are enabled by the embedded/IoT operating system, if applicable.	✓	✓	✓	R6
V7.3	Verify that on-chip debugging interfaces such as JTAG or SWD are disabled or that available protection mechanism is enabled and configured appropriately.	✓	✓	✓	R7
V7.4	Verify that trusted execution is implemented and enabled, if available on the device SoC or CPU.	✓	✓	✓	R8
V7.5	Verify that sensitive data, private keys and certificates are stored securely in a Secure Element, TPM, TEE (Trusted Execution Environment), or protected using strong cryptography.	✓	✓	✓	R9
V7.6	Verify usage of cryptographically secure pseudo-random number generator on embedded device (e.g., using chip-provided random number generators).		✓	✓	R10
V7.7	Verify that sensitive traces are not exposed to outer layers of the printed circuit board.			✓	R11
V7.8	Verify that inter-chip communication is encrypted (e.g. Main board to daughter board communication).			✓	R12

V7.9	Verify the device uses code signing and validates code before execution.			✓	R13
V7.10	Verify that sensitive information maintained in memory is overwritten with zeros as soon as it is no longer required.			✓	R14
V7.11	Verify that the firmware apps utilize kernel containers for isolation between apps.			✓	R15
V7.12	Verify that secure compiler flags such as -fPIE, -fstack-protector-all, -Wl,-z,noexecstack, -Wl,-z, noexecheap are configured for firmware builds.			✓	R16
V7.13	Verify that micro controllers are configured with code protection.			✓	R17
1.1.8 Secure development environment and procedures					
Control-8: Secure development environment and procedures should be applied to the development of IoT systems.					
V8.1	Verify that any use of banned C functions are replaced with the appropriate safe equivalent functions.	✓	✓	✓	R18
V8.2	Verify that each firmware maintains a software bill of materials cataloguing third-party components, versioning, and published vulnerabilities.	✓	✓	✓	R19
V8.3	Verify all code including third-party binaries, libraries, frameworks are reviewed for hardcoded credentials (backdoors).	✓	✓	✓	R20
V8.4	Verify that any available Intellectual Property protection technologies provided by the chip manufacturer are enabled.		✓	✓	R21
V8.5	Verify that only micro controllers that support disabling debugging interfaces (e.g. JTAG, SWD) are used.			✓	R22
V8.6	Verify that only micro controllers that provide substantial protection from de-capping and side channel attacks are used.			✓	R23
1.1.9 Security of IoT systems in support of safety					
Control-9: Security principles in support of safety should be applied to the development of IoT systems.					
V9.1	Ensure the integration of security measures into IoT device development to maintain safety, including mechanisms to detect and halt erroneous or corrupted control data to prevent malfunctions.			✓	R24
1.1.10 Security in connecting varied IoT devices					
Control-10: An IoT system should be designed and implemented to ensure and maintain security in connecting varied IoT devices.					
V10.1	Verify that the firmware apps protect data-in-transit using transport layer security.	✓	✓	✓	R25

V10.2	Verify that the firmware apps validate the digital signature of server connections.	✓	✓	✓	R26
V10.3	Verify that wireless communications are mutually authenticated.	✓	✓	✓	R27
V10.4	Verify that wireless communications are sent over an encrypted channel.	✓	✓	✓	R28
V10.5	Verify that the firmware apps pin the digital signature to a trusted server(s).		✓	✓	R29
1.1.11 Verification of IoT devices and systems design					
Control-11: Design and implementation of IoT devices and IoT systems should be verified.					
Not Applicable for IoT Device Assessment (Applicable for IoT Ecosystem)					
1.1.12 Monitoring and logging					
Control-12: States, events and network traffic of IoT devices and systems should be monitored and logged.					
V.12.1	Ensure that states, events, and network traffic of IoT devices are monitored and logged.			✓	R30
1.1.13 Protection of logs					
Control-13: Logs for IoT devices and systems should be protected from leakage, destruction and unintended alteration.					
V.13.1	Validate that logs for IoT devices are protected from leakage, destruction, and unintended alteration.			✓	R31
V13.2	Verify the presence of tamper resistance and/or tamper detection features.		✓	✓	R32
1.1.14 Use of suitable networks for the IoT systems					
Control-14: Applied network and communication technologies for IoT and systems should meet the needs of communication function, capacity and security, and of function and performance of IoT devices.					
Not Applicable for IoT Device Assessment (Applicable for IoT Ecosystem)					
1.1.15 Secure settings and configurations in delivery of IoT devices and services					
Control-15: IoT devices and services should be delivered with secure settings and configurations.					
V.15.1	Verify that IoT devices are delivered with secure settings and configurations.			✓	R33
V.15.2	Ensure that only authorized entities can modify the configuration settings of the IoT device if they are modifiable.	✓	✓	✓	R34
V.15.3	Verify that IoT devices ensure that common values for critical security parameters, such as global private keys or standard passwords, are replaced by values that are unique per device or explicitly defined by an appropriate external entity before they are put into operation.	✓	✓	✓	R35

V.15.4	Verify security controls are in place to hinder firmware reverse engineering (e.g., removal of verbose debugging symbols).		✓	✓	R36
1.1.16 User and device authentication					
Control-16: Authentication function of users and IoT devices for accessing IoT systems and services should be implemented and applied.					
V.16.1	Confirm the implementation and application of authentication mechanisms for IoT devices accessing IoT systems and services.			✓	R37
V16.2	Verify that IoT devices protect stored and transmitted data, including configuration settings, identifying data, user data, event logs, and sensitive security parameters against unauthorized access, modification, and disclosure, while also safeguarding software from unauthorized access and modification, utilizing cryptography for data confidentiality and integrity.	✓	✓	✓	R38
V16.3	Verify that the application and firmware components are not susceptible to OS Command Injection by invoking shell command wrappers, scripts, or that security controls prevent OS Command Injection.	✓	✓	✓	R39
1.1.17 Provision of software and firmware updates					
Control-17: Mechanism for updating software and firmware of IoT devices and systems should be designed, implemented and operated.					
V17.1	Ensure that the update procedure is defined and includes validation of updates, configuration choices for automatic/manual updates, scheduling options, and notification settings.	✓	✓	✓	R40
V17.2	Ensure that software updates for IoT devices are securely initiated by authorized entities and that interruptions during updates minimize potential harm.	✓	✓	✓	R41
V17.3	Verify that the firmware update process is not vulnerable to time-of-check vs time-of-use attacks.		✓	✓	R42
V17.4	Verify the device uses code signing and validates firmware upgrade files before installing. The update should verify the cryptographic chain of trust with the root of trust.		✓	✓	R43
V17.5	Verify that the device cannot be downgraded to old versions (anti-rollback) of valid firmware.		✓	✓	R44
1.1.18 Sharing vulnerability information					
Control-18: Vulnerabilities of IoT devices, systems and services should be monitored and informed to the IoT users and relevant parties along with associated risks.					

V.18.1	Ensure that vulnerabilities of IoT devices are actively monitored and reported to IoT users and relevant parties along with associated risks.			✓	R45
1.1.19 Security measures adapted to the life cycle of IoT system and services					
Control-19: Security measures of the IoT system and service should be adapted to and kept during the stages of the life cycle, including their development, operation, maintenance and destruction.					
V19.1	Verify that the device wipes firmware and sensitive data upon detection of tampering or receipt of invalid message.			✓	R46
1.1.20 Guidance for IoT users on the proper use of IoT devices and services					
Control-20: The IoT users should be provided with guidance on the proper use of IoT devices with risks and undesirable effects of IoT system and service that can be derived from improper use of IoT devices.					
V.20.1	Verify that IoT users are provided with guidance on the proper use of IoT devices, including risks and potential undesirable effects.			✓	R47
1.1.21 Determination of security roles for stakeholders					
Control-21: Roles of IoT service developer, IoT service provider and other stakeholders in security of IoT system and service should be determined and agreed among relevant parties.					
Not Applicable for IoT Device Assessment (Applicable for IoT Ecosystem)					
1.1.22 Management of vulnerable devices					
Control-22: Vulnerable IoT devices should be detected, recorded, and alerts provided to IoT users and administrators of these devices.					
Not Applicable for IoT Device Assessment (Applicable for IoT Ecosystem)					
1.1.23 Management of supplier relationships in IoT security					
Control-23: Specifications and supporting obligations of suppliers for information security of IoT device and IoT service should be managed by the acquiring organization based on the contracts with suppliers.					
V.23.1	Ensure that the acquiring organization has a system in place to evaluate supplier security measures according to local laws and regulations.	✓	✓	✓	R48
1.1.24 Secure disclosure of Information regarding security of IoT devices					
Control-24: Information on the IoT device relevant to security of IoT services should be documented and disclosed only to the parties that require them.					
V.24.1	Ensure that documentation detailing IoT device security information is present and restrict disclosure solely to pertinent parties.			✓	R49
1.2 Security controls for IoT user					
1.2.1 Contacts and support service					
Control-25:IoT users should only choose IoT devices and IoT services that provide contact information for support service.					
Not Applicable for IoT Device Assessment (Applicable for IoT Ecosystem)					

1.2.2 Initial settings of IoT device and service					
Control-26: Initial settings of IoT device and service should be applied correctly.					
Not Applicable for IoT Device Assessment (Applicable for IoT Ecosystem)					
1.2.3 Deactivation of unused devices					
Control-27: IoT devices should be deactivated and credentials revoked when they are no longer in use.					
Not Applicable for IoT Device Assessment (Applicable for IoT Ecosystem)					
1.2.4 Secure disposal or re-use of IoT device					
Control-28: Data and licensed software stored in IoT device should be removed or securely overwritten prior to disposal or re-use.					
V.28.1	Ensure that data and licensed software stored in IoT device are removed or securely overwritten prior to disposal or re-use.			✓	R50
V.28.2	Verify the IoT device has a secure function allowing only authorized entities to delete relevant user data stored on the device in any memory type.	✓	✓	✓	R51
2. Privacy Controls					
2.1 Privacy controls for IoT service developer and IoT service provider					
2.1.1 Prevention of privacy invasive events					
Control-29: Privacy enhancing capabilities should be built in the IoT devices and IoT services.					
V.29.1	Audit the IoT device to confirm the incorporation of privacy-enhancing features.			✓	R52
2.1.2 IoT privacy by default					
Control-30: Stakeholders in an IoT system should ensure that without any IoT user interaction or intervention, the strictest privacy settings apply by default.					
V.30.1	Ensure that stakeholders of IoT device ensure the strictest privacy settings by default without requiring IoT user interaction or intervention.			✓	R53
2.1.3 Provision of privacy notice					
Control-31-1: The IoT user should be provided with a privacy notice which states personal data collected by the IoT device and IoT service and purpose of its use.					
V.31.1.1	Confirm that IoT users are provided with a privacy notice detailing the collection of personal data by IoT devices and the purpose of its use.			✓	R54
Control-31-2: Consent of the IoT user to the privacy notice should be obtained before collecting the personal data or changing the purpose of use.					
V.31.2.1	Verify that the consent to privacy notice is obtained from IoT users before data collection by IoT device or changes in use.			✓	R55
2.1.4 Verification of IoT functionality					
Control-32: Independent verification of IoT device, data components and IoT service components should be supplied to provide visibility and assurance to all stakeholders that the IoT device or service is operating as per stated objectives.					

Not Applicable for IoT Device Assessment (Applicable for IoT Ecosystem)					
2.1.5 Consideration of IoT users					
Control-33: End users' privacy requirements and concerns should be addressed in designing the IoT device and service.					
V.33.1	Validate that end users' privacy requirements and concerns are addressed in the design of IoT devices.			✓	R56
2.1.7 Management of IoT privacy controls					
Control-34: The effectiveness of privacy controls in the IoT device and service should be reviewed, and new privacy risks be identified on a continuous basis considering the evolving privacy needs of end users and regulatory requirements.					
V.34.1	Obtain a declaration from the IoT device developer confirming regular review of privacy controls' effectiveness and continuous identification of new privacy risks.	✓	✓	✓	R57
2.1.8 Unique device identity					
Control-35-1: IoT system developers (especially device developers) should use a method that uniquely identifies each IoT device to improve privacy for identifying IoT device suspected to be relevant to a cyber incident.					
V35.1.1	Ensure that unique cryptographic keys and certificates are assigned to each individual IoT device to enhance privacy and aid in identifying devices relevant to cyber incidents.	✓	✓	✓	R58
Control-35-2: IoT service providers should use, if required, a method to allow a unique mapping between a given IoT device and an IoT user to improve privacy for identifying the mapping between IoT device and IoT user(s).					
V35.2.1	Ensure a documented process exists to map device identifiers to specific individuals or user profiles for IoT devices. This mapping should be securely maintained and accessible solely by authorized IoT users.			✓	R59
2.1.9 Fail-safe authentication					
Control-36: The system should ensure that implemented authentication cannot be bypassed, tampered, or falsified in any reasonable method.					
V36.1	Verify IoT devices enforce authorized access to interfaces with proper authentication and resist any attempts to bypass, tamper with, or falsify implemented authentication measures.	✓	✓	✓	R60
2.1.10 Minimization of indirect data collection					
Control-37: Collection of data from indirect sources should be minimized or not collected at all.					
V37.1	Verify that IoT devices minimize the collection of indirect data (data collected without user participation) to only what is necessary for operation, unless explicit user consent is obtained.			✓	R61

2.1.11 Communication of privacy preferences					
Control-38: User preferences of privacy controls should be only added, modified, or deleted when the authorized user is authenticated to the system.					
V38.1	Validate that user preferences for privacy controls can only be added, modified, or deleted when the authorized user is authenticated to the IoT device.			✓	R62
2.1.12 Verification of automated decision					
Control-39: Automated decision provided by IoT services should be verified.					
V39.1	Ensure that there is a secondary, independent verification for automated decisions made by IoT devices that could cause irreversible harm to users.			✓	R63
2.1.13 Accountability for stakeholders					
Control-40: Accountability for various stakeholders should be established.					
V40.1	Review documentation to confirm the presence of an accountability framework that outlines data privacy responsibilities for the IoT device.			✓	R64
2.1.14 Unlinkability of PII					
Control-41: The IoT system should ensure that the PII of the user owning a device cannot be identified.					
<<Seek inputs from committee members>>					
2.1.15 Sharing information on PII protection measures of IoT devices					
Control-42: PII protection measures related to privacy risk in IoT devices should be appropriately managed and only disclosed to the parties that require them.					
V42.1	Ensure that PII protection measures related to privacy risk in IoT devices are appropriately managed and only disclosed to the parties that require them.			✓	R65
2.2 Privacy controls for IoT user					
2.2.1 User consent					
Control-43: Consent for use of personal data for the IoT device and service should be provided only after considering the necessity and its probable impact if there is a data breach. Consent should be withdrawn if the IoT output is no longer needed or if there is a concern with the IoT device or service.					
Not Applicable for IoT Device Assessment (Applicable for IoT Ecosystem)					
2.2.2 Purposeful use for connecting with other devices and services					
Control-44: Connection of IoT device and service with other devices or services should be allowed only if there is a valid need.					
Not Applicable for IoT Device Assessment (Applicable for IoT Ecosystem)					
2.2.3 Certification/validation of PII protection					
Control-45: Certification or validation of privacy protection features with respect to the IoT device and service should be sought.					
Not Applicable for IoT Device Assessment (Applicable for IoT Ecosystem)					

Annex A

The security & privacy checkpoints applicable for IoT Devices extracted from the ISO/IEC 27400, ISO/IEC 27402 and OWASP ASVS Appendix C are given below:

Sl. No.	Security & Privacy Checkpoint	L1	L2	L3	Associated Risk
1.	Ensure that a policy for IoT security is defined, approved by management, published, communicated to relevant personnel and relevant external parties and reviewed at planned intervals or if significant changes occur.			✓	R1
2.	Confirm that roles and responsibilities for IoT security are defined and allocated, with accountability clearly established.			✓	R2
3.	Confirm that the IoT device developer has identified all assets across the entire development process of the IoT device.			✓	R3
4.	Ensure that mechanisms are in place to apply knowledge gained from analyzing and resolving IoT device security incidents to reduce the likelihood or impact of future incidents.			✓	R4
5.	Verify that application layer debugging interfaces such USB, UART, and other serial variants are disabled or protected by a complex password.	✓	✓	✓	R5
6.	Verify that memory protection controls such as ASLR and DEP are enabled by the embedded/IoT operating system, if applicable.	✓	✓	✓	R6
7.	Verify that on-chip debugging interfaces such as JTAG or SWD are disabled or that available protection mechanism is enabled and configured appropriately.	✓	✓	✓	R7
8.	Verify that trusted execution is implemented and enabled, if available on the device SoC or CPU.	✓	✓	✓	R8
9.	Verify that sensitive data, private keys and certificates are stored securely in a Secure Element, TPM, TEE (Trusted Execution Environment), or protected using strong cryptography.	✓	✓	✓	R9
10.	Verify usage of cryptographically secure pseudo-random number generator on embedded device (e.g., using chip-provided random number generators).		✓	✓	R10
11.	Verify that sensitive traces are not exposed to outer layers of the printed circuit board.			✓	R11
12.	Verify that inter-chip communication is encrypted (e.g. Main board to daughter board communication).			✓	R12

13.	Verify the device uses code signing and validates code before execution.			✓	R13
14.	Verify that sensitive information maintained in memory is overwritten with zeros as soon as it is no longer required.			✓	R14
15.	Verify that the firmware apps utilize kernel containers for isolation between apps.			✓	R15
16.	Verify that secure compiler flags such as -fPIE, -fstack-protector-all, -Wl,-z,noexecstack, -Wl,-z, noexecheap are configured for firmware builds.			✓	R16
17.	Verify that micro controllers are configured with code protection.			✓	R17
18.	Verify that any use of banned C functions are replaced with the appropriate safe equivalent functions.	✓	✓	✓	R18
19.	Verify that each firmware maintains a software bill of materials cataloguing third-party components, versioning, and published vulnerabilities.	✓	✓	✓	R19
20.	Verify all code including third-party binaries, libraries, frameworks are reviewed for hardcoded credentials (backdoors).	✓	✓	✓	R20
21.	Verify that any available Intellectual Property protection technologies provided by the chip manufacturer are enabled.		✓	✓	R21
22.	Verify that only micro controllers that support disabling debugging interfaces (e.g. JTAG, SWD) are used.			✓	R22
23.	Verify that only micro controllers that provide substantial protection from de-capping and side channel attacks are used.			✓	R23
24.	Ensure the integration of security measures into IoT device development to maintain safety, including mechanisms to detect and halt erroneous or corrupted control data to prevent malfunctions.			✓	R24
25.	Verify that the firmware apps protect data-in-transit using transport layer security.	✓	✓	✓	R25
26.	Verify that the firmware apps validate the digital signature of server connections.	✓	✓	✓	R26
27.	Verify that wireless communications are mutually authenticated.	✓	✓	✓	R27
28.	Verify that wireless communications are sent over an encrypted channel.	✓	✓	✓	R28
29.	Verify that the firmware apps pin the digital signature to a trusted server(s).		✓	✓	R29
30.	Ensure that states, events, and network traffic of IoT devices and systems are monitored and logged.			✓	R30

31.	Validate that logs for IoT devices protected from leakage, destruction, and unintended alteration.			✓	R31
32.	Verify the presence of tamper resistance and/or tamper detection features.		✓	✓	R32
33.	Verify that IoT devices are delivered with secure settings and configurations.			✓	R33
34.	Ensure that only authorized entities can modify the configuration settings of the IoT device if they are modifiable.	✓	✓	✓	R34
35.	Verify that IoT devices ensure that common values for critical security parameters, such as global private keys or standard passwords, are replaced by values that are unique per device or explicitly defined by an appropriate external entity before they are put into operation.	✓	✓	✓	R35
36.	Verify security controls are in place to hinder firmware reverse engineering (e.g., removal of verbose debugging symbols).		✓	✓	R36
37.	Confirm the implementation and application of authentication mechanisms for users and IoT devices accessing IoT systems and services.			✓	R37
38.	Verify that IoT devices protect stored and transmitted data, including configuration settings, identifying data, user data, event logs, and sensitive security parameters, against unauthorized access, modification, and disclosure, while also safeguarding software from unauthorized access and modification, utilizing cryptography for data confidentiality and integrity.	✓	✓	✓	R38
39.	Verify that the application and firmware components are not susceptible to OS Command Injection by invoking shell command wrappers, scripts, or that security controls prevent OS Command Injection.	✓	✓	✓	R39
40.	Ensure that the update procedure is defined and includes validation of updates, configuration choices for automatic/manual updates, scheduling options, and notification settings. The update should maintain the cryptographic chain of trust with the root of trust.	✓	✓	✓	R40
41.	Ensure that software updates for IoT devices are securely initiated by authorized entities and that interruptions during updates minimize potential harm.	✓	✓	✓	R41
42.	Verify that the firmware update process is not vulnerable to time-of-check vs time-of-use attacks.		✓	✓	R42
43.	Verify the device uses code signing and validates firmware upgrade files before installing.		✓	✓	R43

44.	Verify that the device cannot be downgraded to old versions (anti-rollback) of valid firmware.		✓	✓	R44
45.	Ensure that vulnerabilities of IoT devices are actively monitored and reported to IoT users and relevant parties along with associated risks.			✓	R45
46.	Verify that the device wipes firmware and sensitive data upon detection of tampering or receipt of invalid message.			✓	R46
47.	Verify that IoT users are provided with guidance on the proper use of IoT devices, including risks and potential undesirable effects.			✓	R47
48.	Ensure that the acquiring organization has a system in place to evaluate supplier security measures according to local laws and regulations.	✓	✓	✓	R48
49.	Ensure that documentation detailing IoT device security information is present and restrict disclosure solely to pertinent parties.			✓	R49
50.	Ensure that data and licensed software stored in IoT device are removed or securely overwritten prior to disposal or re-use.			✓	R50
51.	Verify the IoT device has a secure function allowing only authorized entities to delete relevant user data stored on the device in any memory type.	✓	✓	✓	R51
52.	Audit the IoT device to confirm the incorporation of privacy-enhancing features.			✓	R52
53.	Ensure that stakeholders of IoT device ensure strict privacy settings by default without requiring IoT user interaction or intervention.			✓	R53
54.	Confirm that IoT users are provided with a privacy notice detailing the collection of personal data by IoT devices and the purpose of its use.			✓	R54
55.	Verify that the consent to privacy notice is obtained from IoT users before data collection by IoT device or changes in use.			✓	R55
56.	Validate that end users' privacy requirements and concerns are addressed in the design of IoT devices.			✓	R56
57.	Obtain a declaration from the IoT device developer confirming regular review of privacy controls' effectiveness and continuous identification of new privacy risks.	✓	✓	✓	R57
58.	Ensure that unique cryptographic keys and certificates are assigned to each individual IoT device to enhance privacy and aid in identifying devices relevant to cyber incidents.	✓	✓	✓	R58
59.	Ensure a documented process exists to map device identifiers to specific individuals or user profiles for IoT devices. This mapping should be securely			✓	R59

	maintained and accessible solely by authorized IoT users.				
60.	Verify IoT devices enforce authorized access to interfaces with proper authentication and resist any attempts to bypass, tamper with, or falsify implemented authentication measures.	✓	✓	✓	R60
61.	Verify that IoT devices minimize the collection of indirect data (data collected without user participation) to only what is necessary for operation, unless explicit user consent is obtained.			✓	R61
62.	Validate that user preferences for privacy controls can only be added, modified, or deleted when the authorized user is authenticated to the IoT device.			✓	R62
63.	Ensure that there is a secondary, independent verification for automated decisions made by IoT devices that could cause irreversible harm to users.			✓	R63
64.	Review documentation to confirm the presence of an accountability framework that outlines data privacy responsibilities for the IoT device.			✓	R64
65.	Ensure that PII protection measures related to privacy risk in IoT devices are appropriately managed and only disclosed to the parties that require them.			✓	R65