EG|CERT

NTRA
National Telecom Regulatory Authority
الجهاز القومي لتنظيم الإتصالات

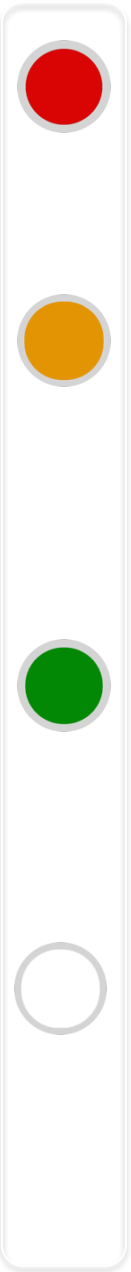
Internet of Things (IoT) Cybersecurity Framework for Critical Infrastructure in the Arab Republic of Egypt

الإطار التنظيمي لتأمين أنظمة إنترنت الأشياء للبنية التحتية الحرجة في جمهورية مصر العربية

نيابة الأمن السيبراني

The Traffic light Protocol (TLP)

The Traffic Light Protocol (TLP) was created in order to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s). The protocol includes four colors (traffic lights), which are detailed as follows:



Red- Not for disclosure, restricted to participants only:
Sources may use TLP: RED when information cannot be effectively acted upon by additional parties. Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed.

Amber- Limited disclosure, restricted to participants' organizations:
Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.

Green- Limited disclosure, restricted to the community:
Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

White- Disclosure is not limited:
Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. TLP: WHITE information may be distributed without restriction.

About Version

EG-SEC-OPER 100-01 Database Policy-V1.2-2308-EN

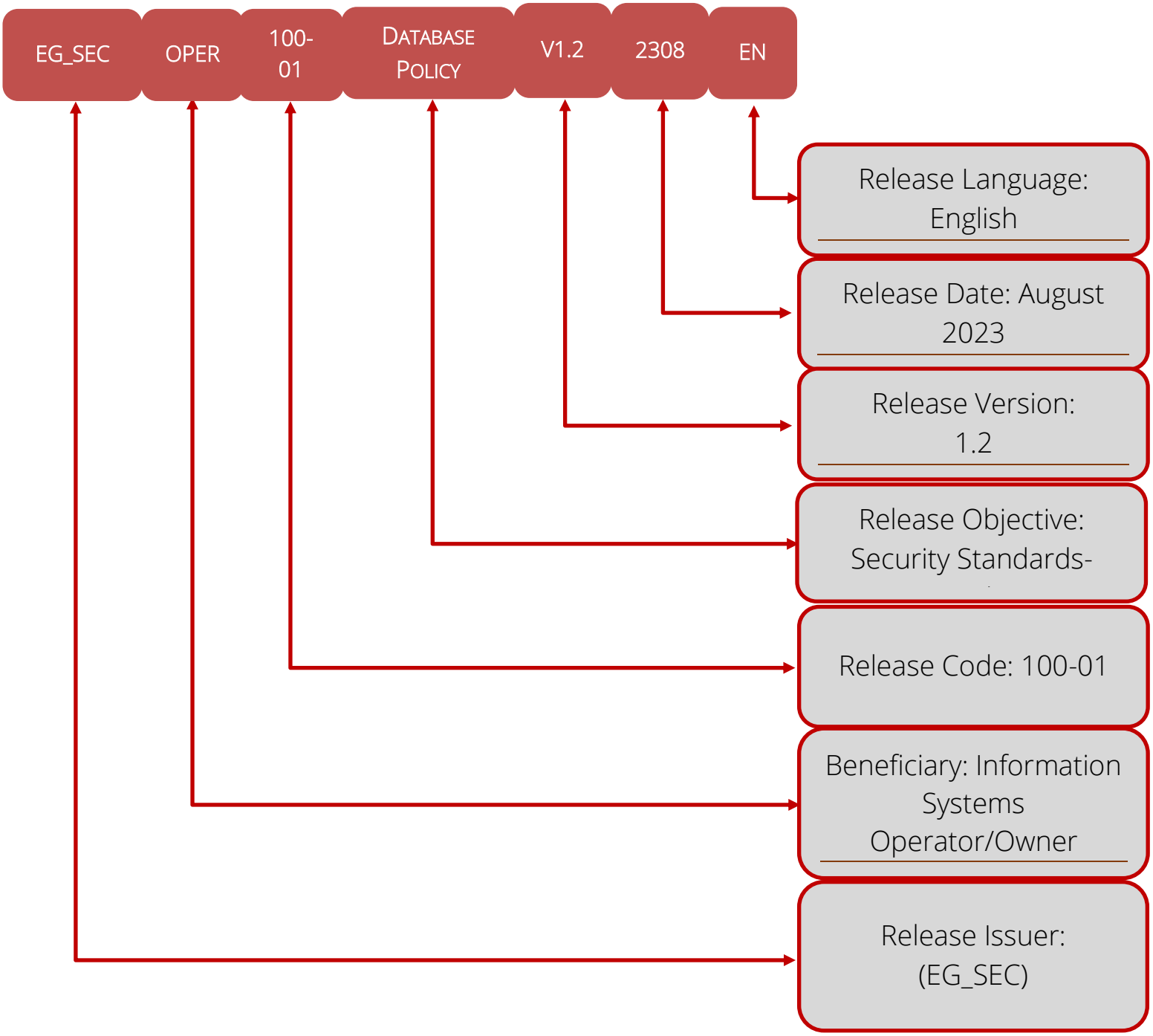


TABLE OF CONTENTS

Contents

INTRODUCTION

OVERVIEW

The Internet of Things (IoT) related products and services have been massively expanding during the last decade. According to reports, there are billions of IoT devices installed worldwide and the number is growing every year, meaning more and more physical devices around the world that are connected to the internet or other networks. Those IoT solutions are very attractive for cyber-attacks due to the amount and type of information and control they possess. It is crucial to protect the IoT devices so people and organizations do not fall victim to cybercrimes.

Due to the extensive proliferation of Internet of Things (IoT) products and services on a global scale, including notable deployment in Egypt, and in alignment with the ARE's 2030 vision which emphasizes the creation of multiple intelligent urban centers akin to the "new administrative capital," the NTRA holds the responsibility of guaranteeing the public and businesses can fully leverage IoT's intelligent offerings while remaining safeguarded against potential cyber threats. Consequently, it has become imperative for the NTRA to establish a foundational set of baseline security guidelines and directives tailored for entities providing IoT services in the ARE. This initiative aims to enhance the security of IoT products, their accompanying services, as well as the confidentiality of consumers and enterprises. These guidelines consider the specific requirements pertinent to the Arab Republic of Egypt.

Furthermore, the integration of operational technologies (OT) into the realm of IoT, particularly for applications in critical infrastructure, underscores the imperative need to meticulously address the cybersecurity measures governing this category of technology. The potential cyber threats in this context hold the capacity to inflict detrimental consequences not only on a nation's security but also on human lives.

The NTRA (National Telecom Regulatory Authority) is the official authority for communication sector regulations in the Arab Republic of Egypt (ARE), that is responsible for providing certifications and approvals for companies and organizations willing to provide communication related solutions and services.

The NTRA has studied the most effective IoT security and cyber security standards, guidelines and frameworks in the world that are relevant, applicable, and effective in the ARE.

And decided to provide these IoT technical security guidelines in the ARE, according to law 10 of year 2003 about telecom regulation. These guidelines bring together most effective IoT security guidelines and cyber security assurance processes, in a sincere attempt to help IoT service providers in securing their products and services by following a complete set of security guidelines, activities and processes provided. Which ensures compliance with the baseline security controls and requirements, and thus mitigating most known attacks in their IoT products and services. The target is to make consumer people and organizations benefit from their IoT devices and services securely, safely, and privately.

This document is complementary to the IoT Framework in the Arab Republic of Egypt document published by the Egyptian NTRA, which can be found in the following web page: https://www.tra.gov.eg/en/regulations/regulatory-framework/iot-regulatory-framework/.

The document follows the executive regulations of law 175 of year 2018 regarding Combating information technology crimes, according to the Egyptian prime minister's decision number 1699 of year 2020.

OBJECTIVE

The IoT cybersecurity framework detailed within this document presents a security assurance procedure, complemented by fundamental security prerequisites and controls, aimed at evaluating and reinforcing the security of the highlighted IoT/OT solutions. The process adheres to established, globally recognized IoT cybersecurity standards and guidelines, ensuring reliability and consistency.

These framework aims to:

- Promote the incorporation of security and privacy prerequisites across IoT solutions and services tailored for critical infrastructure needs, among IoT/OT service providers.
- Provide a set of baseline security requirements and controls which should enhance security of IoT solutions.
- Provide organized and well-defined procedures for IoT service providing organizations to assess their IoT solutions security compliance with the baseline requirements.
- Provide a complete IoT security compliance questionnaire checklist sheet to simplify the security assessment process of the IoT solution of concern for the IoT service providers.
- Guarantee integrity, privacy, and accessibility of IoT products and services designed for critical infrastructure use, benefiting both organizations and end users within the ARE.

TARGET AUDIENCE

IoT service provider organizations running, deploying, operating, providing, or intending to run, deploy, operate, provide IoT device, system, service, solution for critical infrastructure applications within the ARE who are subjected to consider the IoT security guidelines provided in this document.

IoT Service Providers: Companies and organizations that provide services and solutions required by the IoT system to operate. This includes networks, cloud storage, data transfer and any other service required for the full IoT solution.

DISCLAIMER

This document presents a set of procedures and activities that will be carried out by the designated service provider. The objective is to ascertain the robust security posture of the subject IoT solution, aligning it suitably with the requirements of the designated application.

It is crucial to emphasize that this document holds a pivotal role within the ambit of the designated IoT/OT cybersecurity framework. It is important to note that the document, in its current manifestation, remains an ongoing endeavor, with dedicated efforts focused on achieving its final iteration. The forthcoming complete version will encompass a broader spectrum of sections, addressing facets such as network security and the architecture of security mechanisms.

It is the responsibility of the service provider which is using this framework to carry out the IoT Security Assurance Process to ensure the following:

1. They must reach a well understanding of the IoT solution under investigation and the application and sectors into which the IoT solution is deployed.
2. They must ensure providing realistic and genuine information and evaluations whenever required during the process.
3. They must ensure honesty and professionalism during the process and while answering the questionnaire.

Any attempt to provide imperfect or misleading information or unrealistic evaluations that may result in reaching inaccurate results must not be tolerated. And the NTRA security committee has all the rights to request repeating or re-evaluating any of the security assurance process activities or steps to provide more accurate and realistic

information and evaluations to fit criticality of the IoT solution and the application into which it will be deployed.

DOCUMENT STRUCTURE

The remainder of this document consists of the following sections and appendices:

- The Definitions and Acronyms used in this document are presented.
- Then the complete IoT Security framework is provided.
- Followed by the list of tables and list of figures present in the document.
- After that, References used are stated.
- Appendix-A provides a step-by-step complete case study.
- Appendix-B provides the IoT Security Compliance Assessment Questionnaire v1.1. This appendix is attached as a separate document, also as an editable sheet ready to be answered by organizations directly in the sheet.

DEFINITIONS AND ACRONYMS

TERMS AND DEFINITIONS

Attack surface	All possible points (attack vectors), where an unauthorized user can access a system. It is the space that the attacker attacks.
Attack vector	The method which a cyber attacker uses to gain unauthorized access to the system.
IoT vendor	The IoT device manufacturing organization.
IoT service provider	Companies and organizations providing services and solutions required for the IoT system to operate.
IoT device	The hardware devices designed for certain applications, such as sensors, actuators, gadgets, appliances, and other machines, that can collect and exchange data over the Internet or other networks.
OT device	Operational Technology (OT) device is a specialized tool used in industrial settings to monitor and control processes (e.g., sensors, PLCs), with focus on real-time operations and critical infrastructure.
IoT service	The set of services provided by the service provider for the IoT solution, including the ability to connect to the network.
IoT solution	It can be all or any of the following: IoT product, device, system, service, or solution.
The guidelines	Whenever stated in this document, it means the IoT technical security guidelines in the ARE.
Responsible entity	The entity, vendor, or service provider, which is responsible for considering and maintaining a specific security guideline.
Threat	An incident that could harm the system.
Vulnerabilities	The ways in which assets can be exploited.
Risk	The potential for loss or damage when a threat exploits a vulnerability.

ACRONYMS

IoT	The Internet of Things.
OT	Operational Technology
NTRA	The National Telecom Regulatory Authority.
ARE	The Arab Republic of Egypt.
NIST	The National Institute of Standards & Technology.
IoTSF	The Internet of Things Security Foundation.
FIPS	Federal Information Processing Standards.

THE IOT CYBERSECURITY FRAMEWORK

ABOUT THE FRAMEWORK

The objective of this framework is to offer fundamental security directives and requirements for consideration by IoT vendors and service providers. These guidelines merge the most potent considerations for IoT security within the domain, aligning with and adhering to the regulations and security stipulations of the IoT market in the Arab Republic of Egypt.

Table-1 encompasses the set of domains/sectors, obligated to adhere to the processes and comply with security controls outlined within this IoT cybersecurity framework, as described by the executive regulations of law number 175 of year 2018 regarding Combating information technology crimes and the Egyptian NTRA's IoT Framework in the ARE.

The following sections provide a detailed explanation of procedures and steps of activities of the security assurance process along with expected outcomes and required inputs of each one, also the set of responsibilities and commitments of stakeholders through each activity.

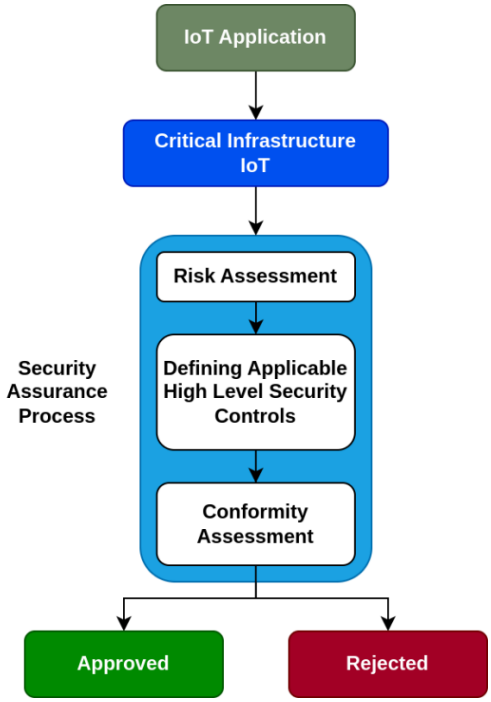


Figure-1: IoT cybersecurity framework main procedures

Category	Domain / Sector	Example IoT Applications
Critical Infrastructure IoT	▪ Energy Sector ▪ Electrical Energy ▪ Health Sector ▪ Natural Gas ▪ Petroleum ▪ Education & Research ▪ Agriculture Sector ▪ Telecom Sector ▪ Financial & Banking Sector ▪ Industrial Sector ▪ Transportation Sector ▪ Radio & TV ▪ Drinking water & Water Resources ▪ Governmental Services ▪ Emergency services ▪ National Security related Information & Communication Services ▪ National Economy related Information & Communication Services	▪ e-Health ▪ Water Management Systems ▪ Electricity Management Systems ▪ Natural Gas Management Systems ▪ Transportation ▪ Education ▪ Smart Cities ▪ Smart Industry Controls ▪ Smart Agriculture

Table-1: IoT Application domains/sectors

IoT SECURITY ASSURANCE PROCESS

The security assurance process provides a set of security requirements for the IoT service providers to comply with. This section describes the IoT security assurance process that the responsible entity should consider in order to assess the security of the IoT product or service under consideration. The responsible entity should consider following this process in order to reach a conclusion determining whether the IoT solution under consideration complies with the baseline security requirements or not.

The assurance process consists of a set of sequential activities, required to be performed by the responsible entity (organization), as briefly explained in figure-2, and then exhaustively explained in figures 3, 4 and 5. It starts by performing a risk assessment activity as explained in figure-3, the outcome of this activity is a risk register; that is an ordered list of applicable risks with a risk score representing impact of each.

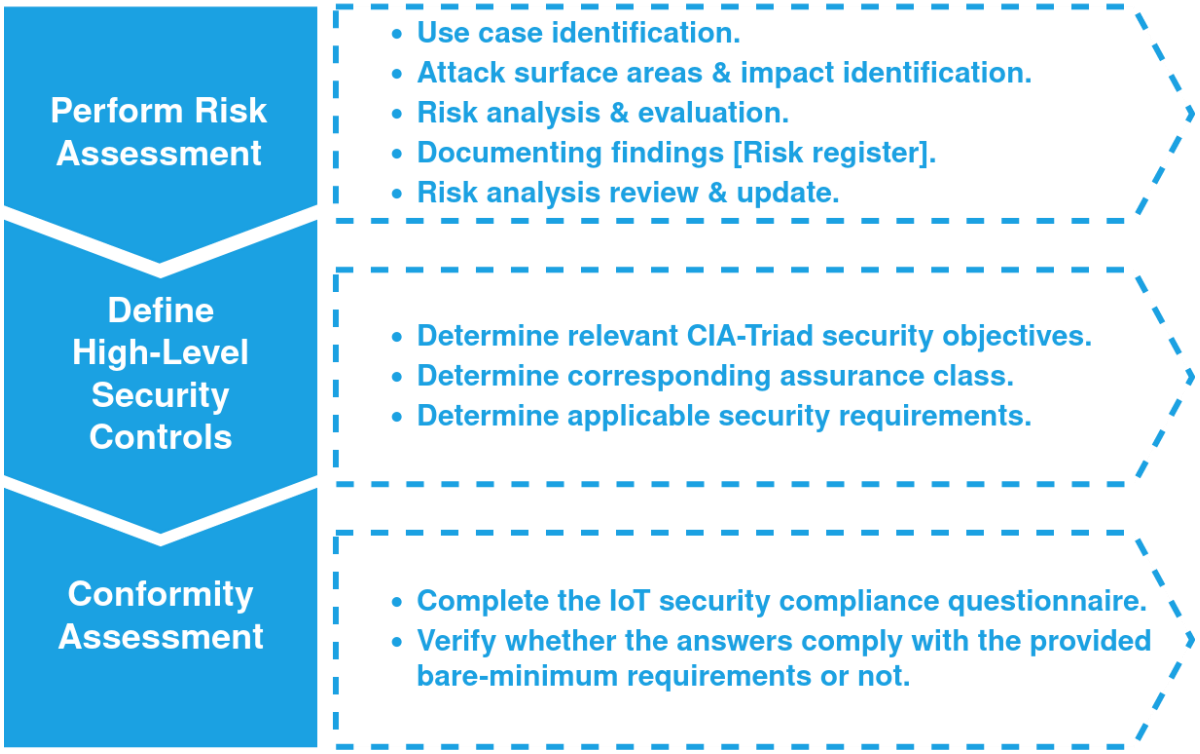


Figure-2: IoT Security assurance process activities Overview

After that, the entity is required to determine the high-level security requirements relevant and applicable for the use cases of concern. Figure-4 explains this activity, where the responsible entity shall use the generated risk register to determine the precise impact for each security objective in the CIA-Triad, then consequently determine the corresponding security class for each; that class is used to relate to the applicable security requirements. Finally, a conformity assessment activity is conducted as described in figure-5; it involves an assessment questionnaire that shall be answered by the entity. Entity should consider answering all questions applicable to the security class determined in the previous step. It should provide reasons and evidence for their answers wherever possible. The resulting checklist clearly determines whether the IoT solution of concern complies with the presented security baseline or not.

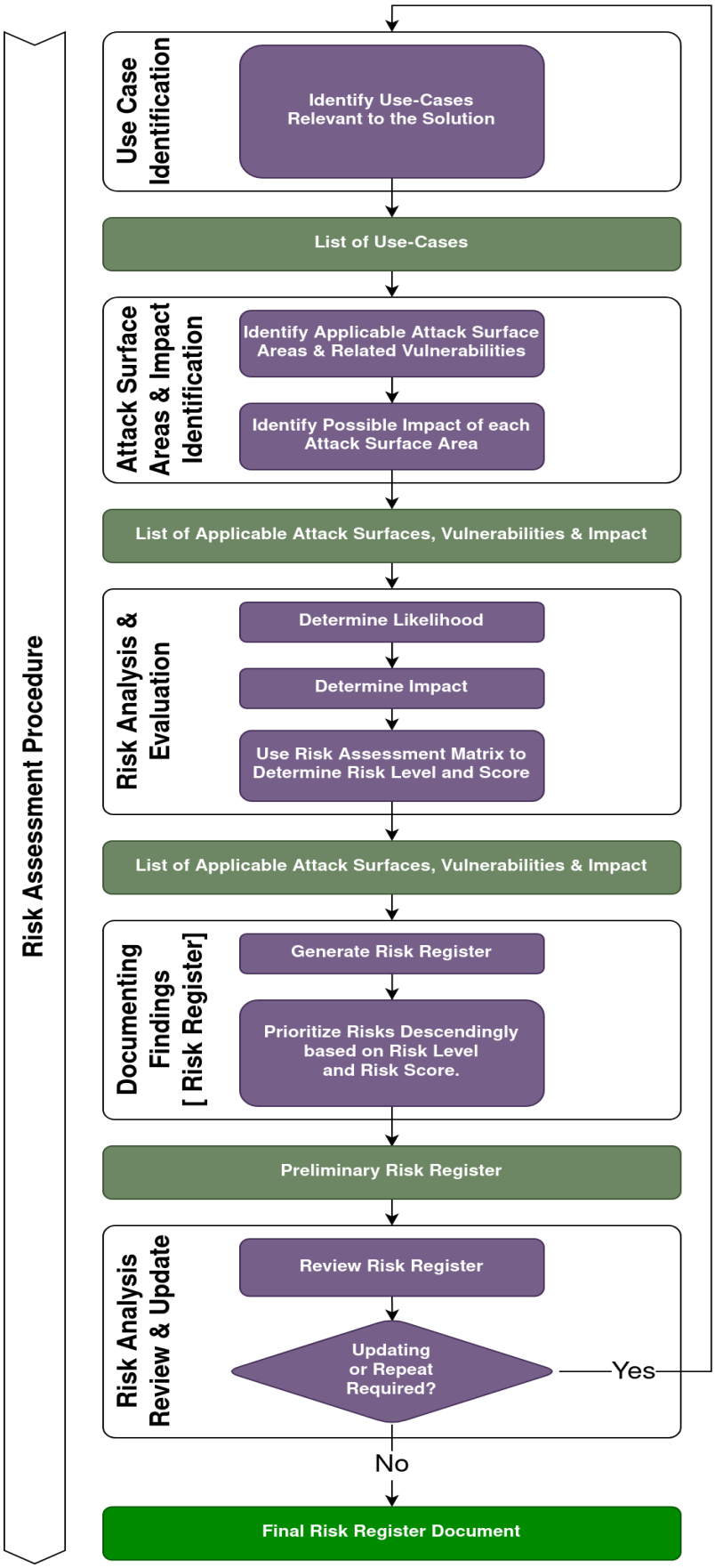


Figure-3: Risk Assessment Procedure

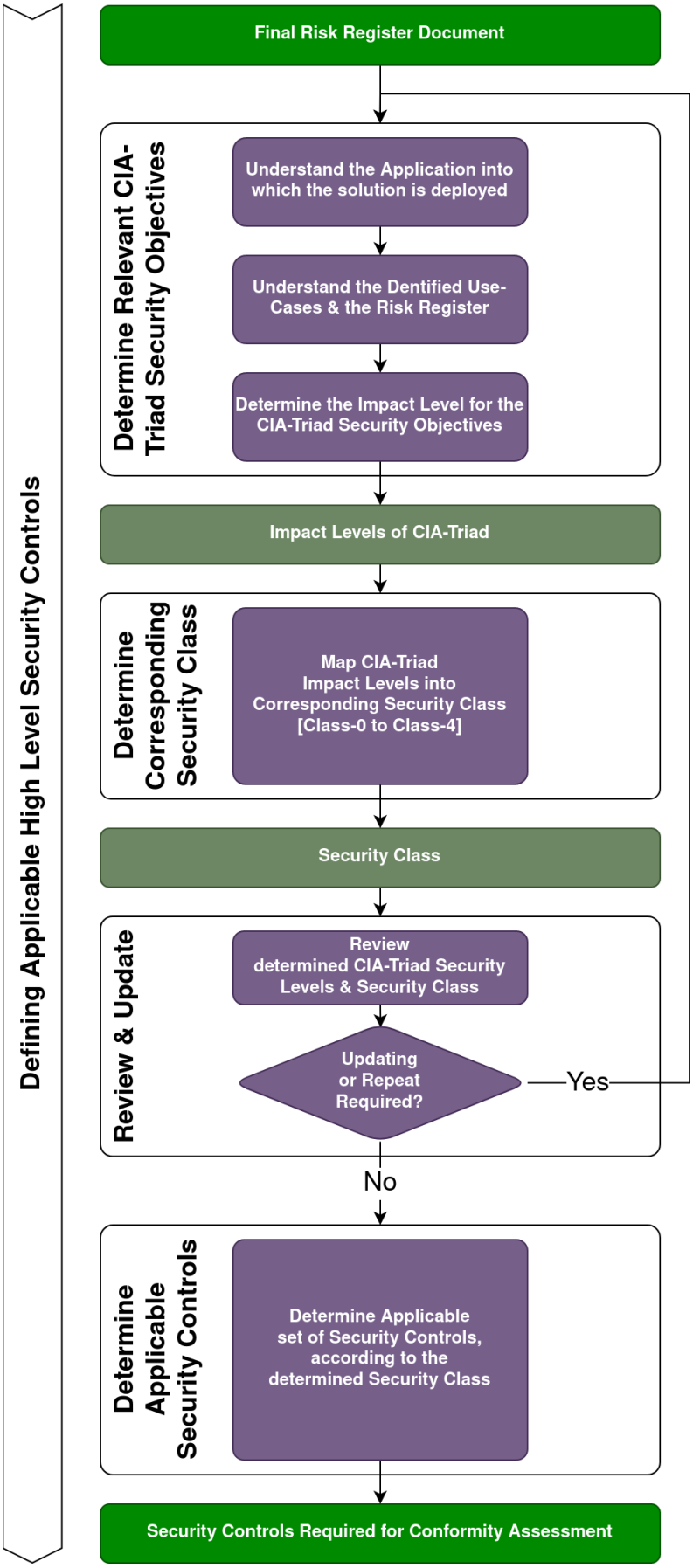


Figure-4: Defining Applicable High Level Security Controls Procedure

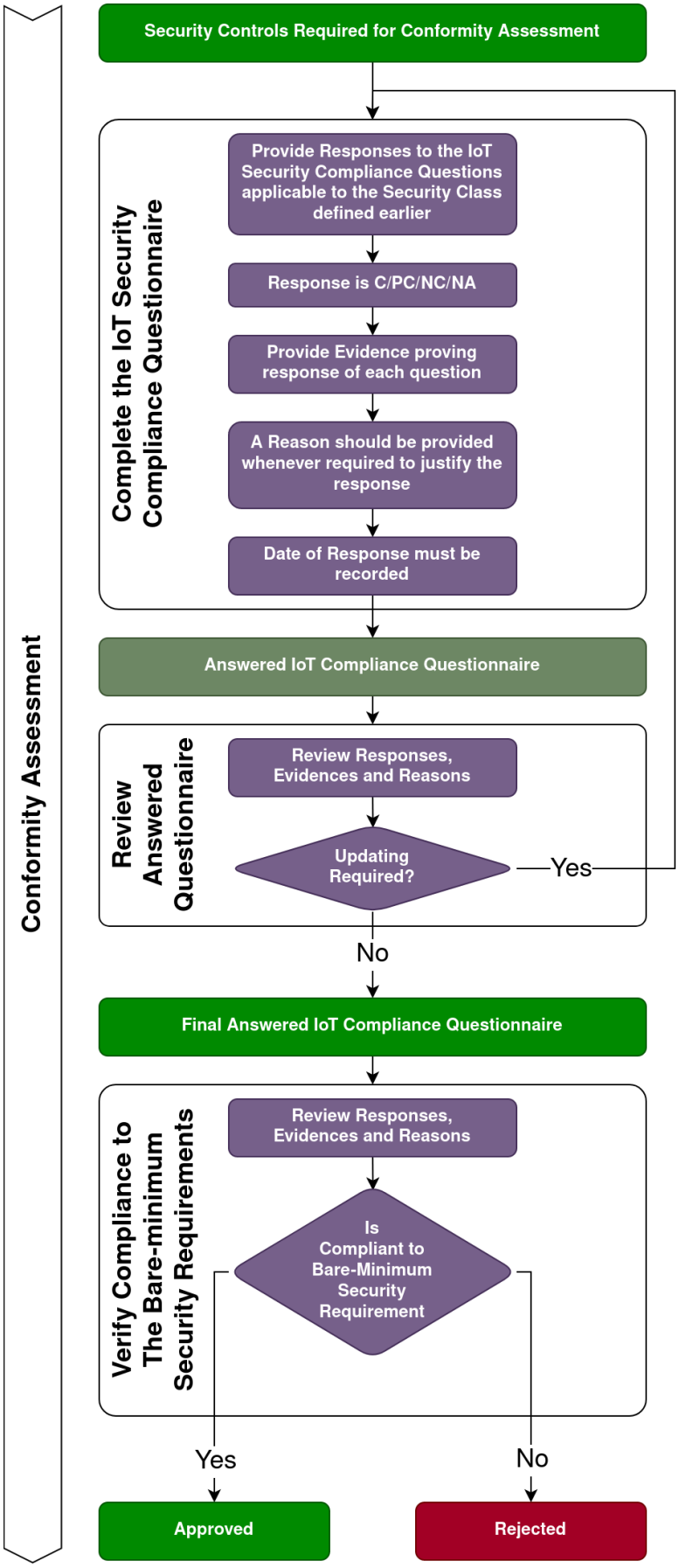


Figure-5: Conformity Assessment Procedure

RISK ASSESSMENT

The risk assessment is the activity of identifying and prioritizing risks to the organizational assets and operations. It is a critical activity as it provides the foundation for the identified risks to be considered. Normally, it is guided by the organization's risk management process. During the ongoing process, IoT security risks are measured and a score for the amount of risk observed is assigned. Figure-6 presents an overview of risk assessment main steps while figure-3 provides a sequential step-by-step flow-graph explaining each step as well as its expected outcome to complete the risk assessment activity.

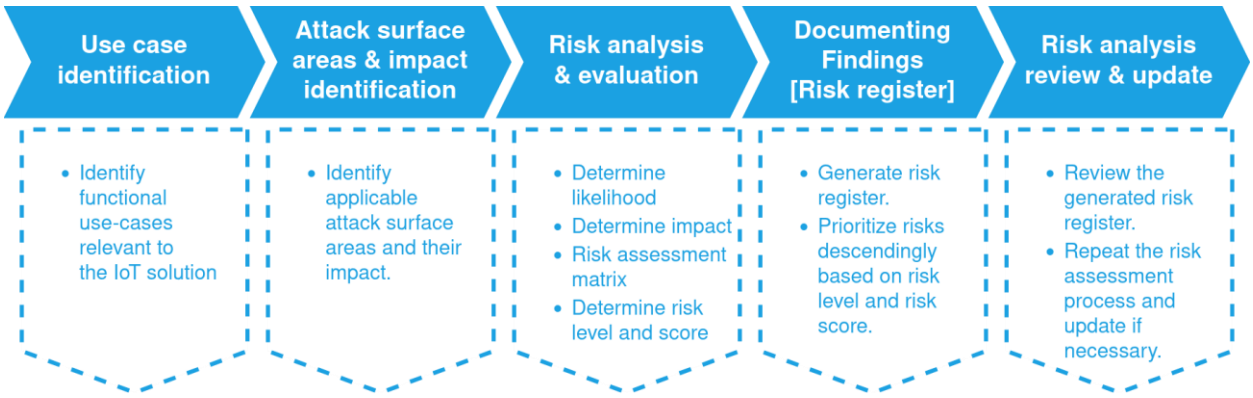


Figure-6: Risk assessment activity main steps

The outcome of this activity is a comprehensive report that can support the risk management team in their decision making. By evaluating possible security threats and vulnerabilities over modules of the IoT solution mainly based on their likelihood of occurrence and impact they could have on the system, then prioritizing them in order to define most effective threats and less effective ones. This outcome is mandatory for the next step, as it is used to determine the relevant CIA-Triad objectives and, consequently, the corresponding security class, and related applicable security requirements, as will be explained in later sections.

This will help the organizations, based on the characteristics of their IoT solution, identify and mitigate the impact of security threats. By determining which risks are applicable and must be treated, and which risks are applicable but could be skipped; this is done in a prioritized

manner having high risk threats on top of the organization's focus going down to the least risky ones. By carrying out this activity, organizations can examine their assets considering the attacker's perspective.

Risk assessment is a general concept that is commonly found in cyber security as well as the business field. Many techniques have been provided to conduct a risk assessment including some well-known risk management standards, e.g., the National Institute of Standards & Technology (NIST) "guide for conducting risk assessments" (NIST standard SP 800-30r1), it is recommended to revise the NIST standard SP 800-30r1 for better understanding. The risk assessment process provided in this document follows main steps presented by the NIST standard SP 800-30r1, which is one of the most reliable related standards.

As explained in figure-3, each step depends on the outcome of its previous step, so each one must be conducted in the described sequence. Starting by identifying the use cases of interest, then defining the applicable attack surface areas, vulnerabilities, and their impact. Followed by performing a risk analysis and evaluation of the considered threats and vulnerabilities. After that, a risk register of the resulting risk factors and scores is formulated and documented. And finally, the risk analysis output document is reviewed for reaching a decision. These steps may be repeated if required, e.g., if the review step found that output is not clear or not enough to conduct a decision.

USE CASE IDENTIFICATION

This is the first step in the risk assessment process, in which organizations are required to identify and document the functional use cases relevant to the IoT solution, representing functionality and services provided, and their associated assets and attributes that could be of interest to attackers.

The outcome of this step is a list of detailed use cases of interest and it is the base for the following steps; in which attack surface areas,

vulnerabilities and their impact that are relevant to each defined use case are carefully identified. An example is provided in the case study at Appendix-B.

ATTACK SURFACE AREA AND IMPACT IDENTIFICATION

An attack surface is the medium that is a part of the system that is susceptible to hacking. This involves all points of access (attack vectors) that an attacker or unauthorized person could use to hack into the IoT system to manipulate data or extract data from the system. It is the space that the attacker attacks. It is recommended to keep the attack surface as small as possible; this makes it easier to protect against attacks.

In order to carry out a risk assessment over the identified list of use cases of interest, from the preceding step, organization is required to identify the set of IoT attack surface areas that are applicable over each use case. Identifying attack surface areas, vulnerabilities and their impact is a base for the risk evaluation to be conducted, as described in the coming up step.

Table-2 presents possible IoT attack surfaces, related vulnerabilities and their impact. It can be used by the responsible entity to identify which attack surface areas are applicable for the product/service under investigation. According to the OWASP IoT project [OWASP-IoT, IoT Attack Surface Areas OWASP. There are about 16 possible IoT attack surfaces according to OWASP.

Attack Surface	Vulnerabilities	Possible Impact
1. Hardware (Sensors)	▪ Sensing Environment Manipulation. ▪ Tampering (Physically). ▪ Damage (Physically).	▪ Inject false reading. ▪ Steal the device. ▪ Update the firmware with malicious code and take control of the device.
2. Device Firmware	▪ Sensitive data exposure (backdoor accounts, hardcoded credentials, encryption keys, sensitive information).	▪ Access the secret keys, user credentials and organization credentials.

Attack Surface	Vulnerabilities	Possible Impact
	▪ Firmware version display and/or last update date. ▪ Vulnerable services (web, ssh, tftp, etc.). ▪ Security related function API exposure. ▪ Firmware downgrade possibility.	▪ Unauthorized access to the IoT system. ▪ Gain sensitive information about the firmware. ▪ Get sensitive URLs. ▪ Create backdoor accounts through the firmware.
3. Device Memory	▪ Sensitive data (Cleartext usernames, cleartext passwords, encryption keys).	▪ Access security keys. ▪ Unauthorized access through stolen credentials. ▪ Access data gathered by device's sensors. ▪ Ability to decrypt sensitive information and communication using stolen encryption keys.
4. Device Physical Interfaces	▪ Firmware extraction. ▪ User CLI. ▪ Admin CLI. ▪ Privilege escalation. ▪ Reset to an insecure state. ▪ Removal of storage media. ▪ Tamper resistance. ▪ Debug port (UART (Serial), JTAG / SWD). ▪ Device ID/Serial number exposure.	▪ Get device ID. ▪ Privilege escalation. ▪ Device malfunction. ▪ Gain shell access to the OS using physical interfaces. ▪ Modifying the source code control flow graph to do malicious activities. ▪ Attacker gains full control over the device through a hacked admin CLI.
5. Device/Cloud Web Interface	▪ Standard set of web application vulnerabilities (check OWASP Web Top 10, OWASP ASVS, OWASP Testing guide). ▪ Credential management vulnerabilities (Username enumeration, Weak passwords, Account lockout, Known default credentials, Insecure password recovery mechanism. ▪ Transport encryption. ▪ Two-factor authentication.	▪ Exploit the web interface of the device/cloud. ▪ Discover security keys and credentials. ▪ Grant unauthorized access to the IoT system. ▪ Access data transmitted. ▪ Misuse of insecure password recovery mechanisms. ▪ Unauthorized access to the system through cross site scripting.

Attack Surface	Vulnerabilities	Possible Impact
		▪ Malicious code execution on the web interface through XSS exploit.
6. Device Network Services	▪ Information disclosure ▪ User CLI ▪ Administrative CLI ▪ Injection ▪ Denial of Service ▪ Unencrypted Services ▪ Poorly implemented encryption ▪ Test/Development Services ▪ Buffer Overflow ▪ UPnP ▪ Vulnerable UDP Services ▪ DoS ▪ Device Firmware OTA update block ▪ Firmware loaded over insecure channel (no TLS) ▪ Replay attack ▪ Lack of payload verification ▪ Lack of message integrity check ▪ Credential management vulnerabilities (Username enumeration, Weak passwords, Account lockout, Known default credentials, Insecure password recovery mechanism).	▪ Launch DoS, buffer overflow and replay attacks ▪ Prevent the transmission of legitimate data. ▪ Access sensitive data. ▪ Block legitimate Over-the-air (OTA) firmware update. ▪ Analyze network traffic. ▪ Privacy breach. ▪ Integrity breach. ▪ Access network security keys and decrypt the communications. ▪ Grant unauthorized access to the IoT system.
7. Network Traffic	▪ LAN ▪ LAN to Internet ▪ Short range ▪ Non-standard ▪ Wireless (WiFi, Z-wave, XBee, Zigbee, Bluetooth, LoRA) ▪ Protocol fuzzing	▪ Prevent the transmission of legitimate data. ▪ Get sensitive data and information. ▪ Analyze network traffic. ▪ Privacy breach. ▪ Integrity breach.

Attack Surface	Vulnerabilities	Possible Impact
8. Update Mechanism	▪ Update sent without encryption ▪ Updates not signed ▪ Update location writable ▪ Update verification ▪ Update authentication ▪ Malicious update ▪ Missing update mechanism ▪ No manual update mechanism	▪ Get a copy of the firmware. ▪ Inject a rogue firmware update to the device resulting in getting access to sensitive information and modify the code control flow graph.
9. Mobile Application	▪ Implicitly trusted by device or cloud ▪ Username enumeration ▪ Account lockout ▪ Known default credentials ▪ Weak passwords ▪ Insecure data storage ▪ Transport encryption ▪ Insecure password recovery mechanism ▪ Two-factor authentication	▪ Access insecure data storage, log file information and unencrypted traffic. ▪ Misuse an insecure password recovery mechanism and grant credentials.
10. Administrative Interface	▪ Standard set of web application vulnerabilities, (check OWASP Web Top 10, OWASP ASVS, OWASP Testing guide) ▪ Credential management vulnerabilities: (Username enumeration, Weak passwords, Account lockout, Known default credentials, Insecure password recovery mechanism. ▪ Security/encryption options (Logging options, Two-factor authentication, Check for insecure direct object references, Inability to wipe device)	▪ Attackers create a backdoor account to take control over the system. ▪ Access to device logs reveal information about the system and users. ▪ Default credentials allow the hacker to take over the device or service. ▪ Lack of 2FA allows the attacker to take over the device using stolen credentials.
11. Authentication/ Authorization	▪ Authentication/Authorization related values (session key, token, cookie, etc.) disclosure ▪ Reusing of session key, token, etc. ▪ Device to device authentication	▪ Gain unauthorized access to the system. ▪ Take control of the system ▪ Change system parameters and configuration.

Attack Surface	Vulnerabilities	Possible Impact
	▪ Device to mobile Application authentication ▪ Device to cloud system authentication ▪ Mobile application to cloud system authentication ▪ Web application to cloud system authentication ▪ Lack of dynamic authentication	▪ Inject malicious data. ▪ Unauthorized access to the system using a legit account.
12. Local Data Storage	▪ Unencrypted data. ▪ Data encrypted with discovered keys. ▪ Lack of data integrity checks. ▪ Use of static same enc/dec key.	▪ Discover secret credentials. ▪ Access sensitive information. ▪ Modify pre-stored information.
13. Vendor Backend APIs	▪ Inherent trust of cloud or mobile application ▪ Weak authentication ▪ Weak access controls ▪ Injection attacks ▪ Hidden services	▪ Inject false data. ▪ Spy on sensitive data. ▪ Rogue devices can authenticate to the APIs leading to taking down the whole service.
14. Third-party Backend APIs	▪ Unencrypted PII sent ▪ Encrypted PII sent ▪ Device information leaked ▪ Location leaked	▪ Inject false data. ▪ Spy on sensitive data. ▪ Vulnerabilities in backend APIs may lead to privilege escalation, unauthorized access, and information leaks.
15. Privacy	▪ User data disclosure ▪ User/device location disclosure ▪ Differential privacy	▪ Access user’s personal information. ▪ User and organization privacy breaches.

Attack Surface	Vulnerabilities	Possible Impact
16. Ecosystem and Communication	▪ Interoperability standards. ▪ Data governance. ▪ Individual stakeholder risks. ▪ Implicit trust between components. ▪ Enrollment security. ▪ Decommissioning system. ▪ Lost access procedures. ▪ Health checks ▪ Heartbeats ▪ Ecosystem commands ▪ Deprovisioning ▪ Pushing updates	▪ Compromise of the device or its related components. ▪ System wide failure. ▪ Manipulate exchanged commands and messages.

Table-2: IoT attack surfaces, related vulnerabilities and its impact

RISK ANALYSIS AND EVALUATION

This step aims to determine the risk factors of each applicable threat (risk) for use cases of interest. It depends on the list of vulnerabilities identified in the former step, providing each one a risk score which represents how much effect this vulnerability has over the IoT solution. The outcome is a list of risk factor scores for the applicable threats and vulnerabilities to be documented and prioritized in the risk register document in the next step.

Evaluating the risk score (risk factor) of a vulnerability requires considering the likelihood or the probability at which the threat could occur along with its impact and severity over the system or the organization.

Risk analysis is highly subjective, that weights of probability levels and of impact level should be determined by the organization. Thus, the organization is required to formulate their own version of the risk assessment matrix that is a combination of both likelihood and impact levels, which shows the level of risk at each possible combination. To evaluate threats of interest, the organization is required to assess

likelihood (probability) and impact (cost) levels for each, based on their understanding of the use cases and its characteristics.

DETERMINE THE LIKELIHOOD

Likelihood is the probability at which cyber security threat events of interest could happen. The organization should assess the likelihood of threat events while considering the characteristics of the use cases of concern, including capability, intent and targeting. e.g., if the threat event requires capabilities more than what the attackers could have, then they are not expected to initiate that threat.

DETERMINE THE IMPACT

Impact is a measurement of the amount of harm, damage or loss that could be caused if a potential threat event happened. The organization has to determine the impact level caused by threat events of concern, considering characteristics of the threat sources which could initiate the events, identified vulnerabilities.

RISK ASSESSMENT MATRIX AND RISK SCORE

The risk assessment matrix is a combination of both likelihood (probability) and impact (severity) of a vulnerability (or a threat). It is a simple and effective method for organizations to assess the risks of concern by defining its risk level, considering estimated likelihood level of the events occurring and impact level that would result from those events. In quantitative methods, risk levels are commonly calculated as the product of the likelihood and impact levels. However, in qualitative methods, it is evaluated by mapping determined likelihood and impact levels to get the corresponding risk level, e.g., a threat of Low likelihood and moderate impact has an assessed risk level of moderate. The calculated level of risk represents the degree to which the organization is threatened by such events.

Table-3 presents an example of a classic 5x5 risk assessment matrix between risk’s likelihood and impact (consequences/severity) levels. Table-4 describes the risk score range for each risk level rating. Tables

3 and 4 follow concepts provided by the NIST standard SP 800-30r1 of the assessment scale tables (Appendix I, table I-2) and (Appendix I, table I-3) respectively. Table-3 represents risk levels in a qualitative manner, which could be converted into quantitative by mapping respective score ranges provided in table-4. This is a starting point that should be tailored and adjusted by the organization for its specific conditions.

			Impact Level				
			Very Low	Low	Moderate	High	Very High
			Negligible effect	Limited effect	Serious effect	Severe effect	Multiple severe effects
Likelihood	Very High	Almost certain	Very Low	Low	Moderate	High	Very High
	High	Highly likely	Very Low	Low	Moderate	High	Very High
	Moderate	Somewhat likely	Very Low	Low	Moderate	Moderate	High
	Low	Unlikely	Very Low	Low	Low	Low	Moderate
	Very Low	Highly unlikely	Very Low	Very Low	Very Low	Low	Low

Table-3: Risk assessment matrix [5x5 example]

Risk level	Risk score	Description
Very Low	[0-4]	Threat could be expected to have a negligible effect.
Low	[5-20]	Threat could be expected to have a limited effect.
Moderate	[21-79]	Threat could be expected to have a serious effect.
High	[80-95]	Threat could be expected to have a severe or catastrophic effect.
Very High	[95-100]	Threat could be expected to have multiple severe or catastrophic effects.

Table-4: Risk levels and scores for risk assessment matrix described in table-3

Another direct quantitative method for evaluating risk scores, is to multiply the calculated likelihood (probability) value by the calculated impact (cost) value directly. This will produce the risk score as a

quantitative value, which could be mapped into its corresponding risk level using ranges defined in table-4.

DOCUMENT FINDINGS [RISK REGISTER]

After finishing the risk analysis step and providing risk factors and scores of each threat, the organization's team is required to well document the results for review and decision making. The risk register is an appropriate and organized way of documenting these results. The organization should create a risk register document based on the outcomes evaluated in the former step.

This risk register document should include all applicable threats with their associated risk factor scores. In which threat events of concern are ordered descendingly by the level of risk determined earlier, with the highest attention going to high-risk events. Risks of the same risk level can be further prioritized by experience or based on their quantitative risk factor scores. Thus, the risk with the highest risk score should be at the top of the table going down to that of the least score at the bottom. The reason for this prioritization criteria is to guide and justify the word needed for the IoT solution's security. This work shall mainly focus on reducing the risk likelihood (probability) factor to an acceptable level.

Risks with higher risk factors could highly compromise the IoT solution, and must be highly and strictly considered for treatment and mitigation; the organization should assign as many resources as possible to decrease their risk factors. However, risks with lower priority, having lower risk factors, can be postponed or even neglected if their risk factor scores are not significant at all.

An example of a simplified risk register is presented in table-5, however, the risk register document could have more columns with extra information for each considered threat. This is the base for determining the relevant security requirement, as will be explained in later sections.

Threat	Description	Impact	Likelihood	Risk Factor	Risk Level [Output]
Unauthorized access	An attacker could initiate an unauthorized access attack to access the IoT system for monitoring or pushing information.	Very High	Very High	97	**Very High**
Denial of service attack	An attacker attacks the system to prevent devices from accessing the system's network.	High	Very High	88	**High**
Firmware extraction	An attacker dumps the firmware from the IoT device chipset, to extract useful information.	High	Moderate	50	**Moderate**

Table-5: Example of a simplified risk register

RISK ANALYSIS REVIEW AND UPDATE

The last, but not least, step of the risk assessment activity is to review the output risk register document and the whole process output.

If the reviewers noticed any inconsistency of the results regarding the identified use cases, or that threats or use cases are not well identified or not well covering the IoT solution under investigation, the whole process should be repeated and refined to solve found issues.

If the results are well documented and organized, then the document should provide a solid and organized source presenting threats and vulnerabilities relevant to the IoT solution of interest. This shall help the organization in deciding the order of threats by which they should be investigated and mitigated; that higher priority threats should be considered at first and may require higher resources.

The final risk register is used by the following activity; it is the base to determine the proper impact for each security objective according to the CIA-Triad for the IoT solution under investigation, that is consequently used to determine the corresponding security class for the whole solution. The determined security class is the key to determine the relevant security requirements, as described through the next activity.

RESPONSIBILITIES & COMMITMENTS

- It is the responsibility of the service provider to follow all steps of the risk assessment activity and provide appropriate and exact information as required, and to review and provide the final risk register document.
- If requested by the service provider, the NTRA security committee is responsible for auditing the activity output for approval or rejection, with the aim of providing consultation concerning the risk assessment procedure.

HIGH LEVEL SECURITY CONTROLS

OVERVIEW

The target of this section is to determine the required security controls for the IoT application based on the actual use case and the risk assessment. The security controls described in this publication have a well-defined structure based on a risk assessment approach derived from the CIA triad. The controls are organized into 11 domains as described in this document based on 5 security levels according to the IoTSF (*The Internet of Things Security Foundation*) Security Assurance Framework, as described in table-9.

Depending on the use cases, the type of the provided service, the market and the application in which the product is intended to be used, the risk assessment determines the correct level of the security controls which matches the CIA impact level. For example, a home/small office Wi-Fi router used in connecting clients to the internet, could be assessed under impact level 0 where the threat is targeting individuals and is considered a low risk. However, when deploying Wi-Fi in a train signaling control system, it could be assessed under the highest impact level 5 because there is a very high-level threat targeting the train control systems and affecting the passengers' life.

Figure-7 presents an overview of steps required to determine the high level security controls applicable for the IoT solution of concern. While figure-4 presents the sequential steps required to perform this activity with the expected outcome of each step.

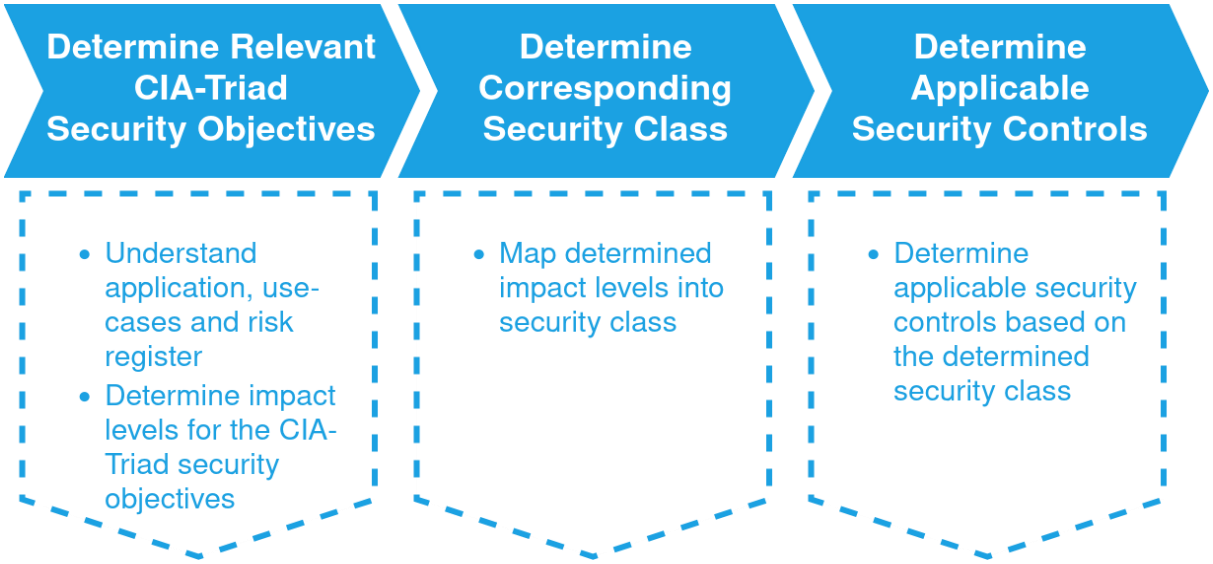


Figure-7: Defining applicable high level security controls procedure

THE CIA TRIAD

Following are definitions for the security objectives of the CIA triad:

- **Confidentiality:**
  - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
  - Unauthorized access or unauthorized information disclosure is considered a violation.
- **Integrity:**
  - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
  - Unauthorized modifications and manipulations are considered a violation.
- **Availability:**
  - Ensuring timely and reliable access to and use of information.
  - Disrupting or denying access to the system or the information is considered a violation.

Based on these definitions, the impact levels are specified in Table-6 as defined in FIPS 199 (*FIPS: Federal Information Processing Standards*), Standards for Security Categorization of Federal Information and Information Systems. These impact levels are used later to determine the required security controls.

Objective	Low Impact	Moderate Impact	High Impact
Confidenti-ality	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Table-6: CIA Triad impact levels explained

In order to apply an appropriate level of security assurance to a service according to the IoTSF Security Framework, where the requirements are classified into the following classes:

Class	Description
Class 0	Where compromise to the data generated or loss of control is likely to result in little discernible impact on an individual or organization.
Class 1	Where compromise to the data generated or loss of control is likely to result in no more than limited impact on an individual or organization.
Class 2	In addition to class 1, the device is designed to resist attacks on availability that would have significant impact on an individual or organization or impact many individuals. For example, by limiting operations of an infrastructure to which it is connected.
Class 3	In addition to class 2, the device is designed to protect sensitive data including Personally identifiable information (PII).
Class 4	In addition to class 3, where compromise to the data generated or loss of control have the potential to affect critical infrastructure or cause personal injury.

Table-7: Security requirement classes for the IoT technical security guidelines

The security requirements classes in table-7 are mapped to the corresponding impact levels of the CIA triad according to table-8.

Class	Confidentiality	Integrity	Availability
Class 0	**L**	**L**	**L**
Class 1	**L**	**M**	**M**
Class 2	**M**	**M**	**H**
Class 3	**H**	**M**	**H**
Class 4	**H**	**H**	**H**

Table-8: Mapping security requirement classes to the CIA impact levels

The following practical example can be used to explain determining the security class. Consider an IoT smart meter connected to the AMI system, the process can be as follows:

1. **Determine the CIA impact:**
   A. **Confidentiality** is **High** since the smart meter stores sensitive data such as the readings and tariff, and the network stores sensitive information about the users and meter controls which

could have catastrophic effect on user privacy and the smart grid network.

B. **Integrity** is **Medium** since poor data integrity can cause readings manipulation resulting in a serious effect on the organization.

C. **Availability** is **High** since a denial of service can cause a complete power outage and is considered catastrophic.

2. Determine the security requirements class:

which is **class 3** in this case.

3. Determine security controls corresponding to the defined security class:

For this case, all security controls marked as the following

1. "Mandatory for class 3 and above"
2. "Mandatory for class 2 and above"
3. "Mandatory for class 1 and above"
4. "Mandatory for all classes"

are all applicable and mandatory requirements which should be considered.

The security technical requirements are organized into 11 Domains according to table-9. These technical requirements describe the required security controls for the service security level from a technical point of view. For example, a service which has a class 4 security requirement must have data encryption quality according to NIST.

Category	Domain	References
Technical requirements	Device Hardware & Physical Security	- NIST SP800-53Ar5 - NIST SP800-213A - IoTSF
	Device Software	
	Device Operating System	
	Device Wired and Wireless Interfaces	
	Authentication and Authorization	
	Encryption and Key Management for Hardware	
	Cybersecurity State Awareness	
	Web User Interface	
	Mobile Application	
	Cloud and Network Elements	
	Continuous assessments and monitor	

Table-9: List of security requirements categories and domains

RESPONSIBILITIES & COMMITMENTS

- It is the responsibility of the service provider to determine impact levels on confidentiality (C), integrity (I) and availability (A) for the solution under investigation, based on the well understanding of the service, the application into which the IoT solution is deployed and the identified use-cases; while providing proper justification, reasoning and evidence supporting the determined impact levels. And thus determining the corresponding security class, according to the CIA triad impact levels approach for robust and clear reasoning. The service provider must always ensure honesty and professionality to provide realistic and genuine evaluation of the IoT solution's CIA-Triad security impact; for ensuring accurate results.
- The NTRA security committee is responsible for auditing the determined CIA objectives, the security class and the corresponding applicable security controls, to ensure that the calculated security controls are of enough and appropriate security levels, in order to fit the criticality of the intended target application.

TECHNICAL REQUIREMENTS

DEVICE HARDWARE AND PHYSICAL SECURITY

The service security includes the IoT device protection (If applicable), communication system protection, and overall system security. This section provides policies and controls required for hardware and physical security of IoT devices. Including requirements to mitigate device impersonation and misconfiguration.

The following table lists these requirements and controls, it follows the IoTSF Security Assurance Framework selected requirements from 2.4.4.1 through 2.4.4.18 and the NIST SP800-53Ar5 selected requirements from CM-02 through CM-08, IA-03, AC-03, SI-04 and SR-11

Req. No	Security Requirements	Security Class
HP-01	The product's processor system has an irrevocable hardware Secure Boot process.	Mandatory for all classes
HP-02	The product's processor system has an irrevocable "Trusted Root Hardware Secure Boot"	Mandatory for Class 2 and above
HP-03	The product's processor boot process provides an appropriate level of trustworthiness by using a hardware root of trust to verify trusted boot or measured boot methods. This may be referred to as 'secure boot', but absolute security cannot be assured.	Mandatory for Class 3 and above
HP-04	The Secure Boot process is enabled by default.	Mandatory for all classes
HP-05	Any debug interface only communicates with authorized and authenticated entities on the production devices. The functionality of any interface should be minimized to its essential task(s).	Mandatory for Class 1 and above
HP-06	The hardware incorporates protection against tampering and this has been enabled. The level of tamper protection must be determined by the risk assessment.	Mandatory for Class 1 and above
HP-07	The hardware incorporates physical, electrical and logical protection against tampering to reduce the attack surface. The level of protection must be determined by the risk assessment.	Mandatory for Class 2 and above

Req. No	Security Requirements	Security Class
HP-08	The hardware incorporates physical, electrical & logical protection against reverse engineering. The level of protection must be determined by the risk assessment.	Mandatory for Class 3 and above
HP-09	All communications port(s) which are not used as part of the product's normal operation are not physically accessible or only communicate with authorized and authenticated entities.	Mandatory for Class 1 and above
HP-10	All the product's development test points are securely disabled or removed wherever possible in production devices.	Mandatory for Class 2 and above
HP-11	Tamper Evident measures have been used to identify any interference to the assembly to the end user.	Mandatory for Class 2 and above
HP-12	In production devices the microcontroller/ microprocessor(s) shall not allow the firmware to be read out of the products non-volatile [FLASH] memory. Where a separate non-volatile memory device is used the contents shall be encrypted.	Mandatory for Class 1 and above
HP-13	Where the product's credential/key storage is external to its processor, the storage and processor shall be cryptographically paired to prevent the credential/key storage being used by unauthorized software.	Mandatory for Class 1 and above
HP-14	Where a production device has a CPU watchdog, it is enabled and will reset the device in the event of any unauthorized attempts to pause or suspend the CPU's execution.	Mandatory for Class 1 and above
HP-15	Where the product has a hardware source for generating true random numbers, it is used for all relevant cryptographic operations including nonce, initialization vector and key generation algorithms.	Mandatory for Class 1 and above
HP-16	The product shall have a hardware source for generating true random numbers.	Mandatory for Class 2 and above
HP-17	The product should have hardware mechanisms to control access to memory to reduce the risk of running malicious code.	Mandatory for Class 3 and above
HP-18	DEVICE IDENTIFICATION AND AUTHENTICATION: 1. devices and/or types of devices to be uniquely identified and authenticated before establishing a connection are defined; 2. device ability to support unique device identifier	Mandatory for all classes
HP-19	Actions Based on Device Identity: 1. Ability to configure IoT device access control policies using IoT device identity. 2. Ability to hide IoT device identity from non-authorized entities. 3. Ability for the IoT device to differentiate between authorized and unauthorized remote users. 4. Ability for the IoT device to differentiate between authorized and unauthorized physical device users (e.g., using a method of authentication to verify the identity of physical device users).	Mandatory for all classes

Req. No	Security Requirements	Security Class
	5. Ability to monitor specific actions based on the IoT device identity. 6. Ability to identify software loaded on the IoT device based on IoT device identity. 7. Ability for the device identifier to be used to discover the IoT device for the purpose of network asset identification and management	
HP-20	Physical Identifiers: 1. Ability to add a unique physical identifier at an external or internal location on the device authorized entities can access.	Mandatory for all classes
HP-21	DEVICE CONFIGURATION: 1. The capability to configure the IoT device through logical and/or physical interfaces to meet organizational requirements.	Mandatory for all classes

Table-10: Device hardware and physical security Policies, and controls

DEVICE SOFTWARE

This section provides a set of policies, controls and considerations required for securing the device software. Including controls for securing remote software updates, communication, memory access, software reversion, sensitive information, inputs and outputs, device boot, configuration, maintenance and storage.

The following table lists these requirements and controls, it follows the IoTSF Security Assurance Framework selected requirements from 2.4.5.1 through 2.4.5.41 and the NIST SP800-53Ar5 selected requirements from CM-02 through CM-07, MA-03, SA-10, CP-9, CP-9(8), MP-06 and SC-28.

Req. No	Security Requirements	Security Class
DS-01	The product has measures to prevent unauthorized and unauthenticated software, configurations and files being loaded onto it. If the product is intended to allow unauthenticated software, such software should only be run with limited permissions and/or sandbox.	Mandatory for all classes
DS-02	Where remote software updates can be supported by the device, the software images must be digitally signed by an appropriate signing authority - e.g., manufacturer/supplier or public. The Signing Authority should be clearly identified.	Mandatory for all classes
DS-03	Where updates are supported, the software update package has its digital signature, signing certificate and signing certificate chain verified by the device before the update process begins.	Mandatory for all classes

Req. No	Security Requirements	Security Class
DS-04	If remote software upgrade is supported by a device, software images shall be encrypted or transferred over an encrypted channel.	Mandatory for Class 2 and above
DS-05	If the product has any virtual port(s) that are not required for normal operation, they are only allowed to communicate with authorized and authenticated entities or are securely disabled when shipped. When a port is initialized or used for field diagnostics, the port input commands are deactivated and the output provides no information which could compromise the device, such as credentials, memory address or function names.	Mandatory for Class 2 and above
DS-06	To prevent the stalling or disruption of the device's software operation, watchdog timers are present, and cannot be disabled.	Mandatory for Class 1 and above
DS-07	The product's software signing root of trust is stored in tamper-resistant memory.	Mandatory for Class 1 and above
DS-08	The product has protection against unauthorized reversion of the software to an earlier and potentially less secure version. Only authorized entities can restore the software to an earlier secure version.	Mandatory for Class 2 and above
DS-09	There are measures to prevent the installation of non-production (e.g., development or debug) software onto production devices.	Mandatory for Class 1 and above
DS-10	Production software images shall be compiled in such a way that all unnecessary debug and symbolic information is removed, to prevent accidental release of superfluous data.	Mandatory for Class 1 and above
DS-11	Development software versions have any debug functionality switched off if the software is operated on the product outside of the product vendor's trusted environment.	Mandatory for Class 2 and above
DS-12	Steps have been taken to protect the product's software from sensitive information leakage, including at network interfaces during initialization, and side-channel attacks.	Mandatory for Class 3 and above
DS-13	The product's software source code follows the basic good practice of a language subset coding standard.	Mandatory for Class 2 and above
DS-14	The product's software source code follows the basic good practice of static vulnerability analysis by the developer.	Mandatory for Class 2 and above
DS-15	The software must be architected to identify and ring fence sensitive software components, including cryptographic processes, to aid inspection, review and test. The access from other software components must be controlled and restricted to known and acceptable operations. For example, security related processes should be executed at higher privilege levels in the application processor hardware.	Mandatory for Class 1 and above
DS-16	Software source code is developed, tested and maintained following defined repeatable processes.	Mandatory for Class 1 and above

Req. No	Security Requirements	Security Class
DS-17	The build environment and toolchain used to compile the application is run on a build system with controlled and auditable access.	Mandatory for Class 2 and above
DS-18	The build environment and toolchain used to create the software is under configuration management and version control, and its integrity is validated regularly.	Mandatory for Class 2 and above
DS-19	Where present, production software signing keys are under access control.	Mandatory for all classes
DS-20	The production software signing keys are stored and secured in a storage device compliant to FIPS-140-2/FIPS-140-3 level 2, or equivalent or higher standard.	Mandatory for Class 1 and above
DS-21	Where the device software communicates with a product related web server or application over TCP/IP or UDP/IP, the device software uses certificate pinning or public/private key equivalent, where appropriate.	Mandatory for Class 2 and above
DS-22	For a device with no possibility of a software update, the conditions for and period of replacement support should be clear. A replacement strategy must be communicated to the user, including a schedule for when the device should be replaced or isolated.	Mandatory for all classes
DS-23	All inputs and outputs are checked for validity e.g., use “Fuzzing” tests to check for acceptable responses or output for both expected (valid) and unexpected (invalid) input stimuli.	Mandatory for Class 2 and above
DS-24	The software has been designed to meet the safety requirements identified in the risk assessment; for example, in the case of unexpected invalid inputs, or erroneous software operation, the product does not become dangerous, or compromise security of other connected systems.	Mandatory for Class 2 and above
DS-25	Support for partially installing updates is provided for devices whose on-time is insufficient for the complete installation of a whole update (constrained devices).	Advisory for all classes
DS-26	Support for partially downloading updates is provided for devices whose network access is limited or sporadic.	Advisory for all classes
DS-27	Where real-time expectations of performance are present, update mechanisms must not interfere with meeting these expectations (e.g., by running update processes at low priority, or notifying the user of the priority and duration of the update and with the option of postponing or disabling the update).	Mandatory for all classes
DS-28	Where a device doesn’t support secure boot, upon a firmware update the user data and credentials should be re-initialized.	Mandatory for all classes
DS-29	Where a device cannot verify authenticity of updates itself (e.g., due to no cryptographic capabilities), only a local update by a physically present user is permitted and is their responsibility.	Mandatory for all classes
DS-30	An update to a device must be authenticated before it is installed. Where the update fails authentication, the device should, if possible, revert to the last known good (current stable) configuration/software image which was stored on the device.	Mandatory for all classes

Req. No	Security Requirements	Security Class
DS-31	There is secure provisioning of cryptographic keys for updates during manufacture in accordance with industry standards.	Mandatory for Class 1 and above
DS-32	Memory locations used to store sensitive material (e.g., cryptographic keys, passwords/passphrases, etc.) are sanitized as soon as possible after they are no longer needed. These can include but are not limited to locations on the heap, the stack, and statically-allocated storage.	Mandatory for Class 2 and above
DS-33	Any caches which potentially store sensitive material are cleared flushed after memory locations containing sensitive material have been sanitized.	Mandatory for Class 3 and above
DS-34	An end-of-life policy shall be 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. The need for each update should be made clear to users and an update should be easy to implement. At the end of the support period, the device should reduce the risk of a latent vulnerability being exploited. This could be by indicating an error condition to the user or curtailing functionality. This action should be clearly communicated to the user during the procurement stage.	Mandatory for all classes
DS-35	Updates should be provided for a period appropriate to the device, and this period shall be made clear to a user when supplying the device. Updates should, where possible, be configurable to be automatically or manually installed. The supply chain partners should inform the user that an update is required.	Mandatory for all classes
DS-36	The device manufacturer should ensure that shared libraries (e.g., Clib or Crypto libraries) that deliver network and security functionalities have been reviewed or evaluated (note that the actual review or evaluation does not have to be conducted by the manufacturer if it has been conducted by another reputable organization or government entity). Cryptography libraries should be re-reviewed for known security vulnerabilities on each update of the device.	Mandatory for Class 2 and above
DS-37	Maintenance changes should trigger full security regression testing.	Mandatory for Class 2 and above
DS-38	IoT devices must allow software updates to maintain security over the product lifetime.	Mandatory for Class 2 and above
DS-39	Hard-coded critical/ security parameters in device software source code shall not be used; if needed these should be injected in a separate (secure) process.	Mandatory for all classes
DS-40	Where the device is capable, it should check after initialization, and then periodically, whether security updates are available, either autonomously or as part of the support service. Otherwise, the support service should push updates to the device.	Mandatory for Class 1 and above
DS-41	BASELINE CONFIGURATION: 1. automated mechanisms for maintaining baseline configuration of the system are defined; 2. software programs not authorized to execute on the system are defined; 3. frequency at which to review and update the list of unauthorized software programs is defined;	Mandatory for all classes

Req. No	Security Requirements	Security Class
DS-42	MAINTENANCE TOOLS: 1. maintenance tools are inspected to ensure that the latest software updates and patches are installed.	Mandatory for all classes
DS-43	DEVELOPER CONFIGURATION MANAGEMENT: 1. the developer of the system, system component, or system service is required to enable integrity verification of software and firmware components.	Mandatory for all classes
DS-44	Secure Storage: 1. Ability to support encryption of data at rest 2. Ability to cryptographically store passwords at rest, as well as device identity and other authentication data 3. Ability to support data encryption and signing to prevent data from being altered in device storage. 4. Ability to secure data in device storage. 5. Ability to secure data stored locally on the device. 6. Ability to secure data stored in remote storage areas (e.g., cloud, server, etc.). 7. Ability to utilize separate storage partitions for system and user data. 8. Ability to securely back-up the data on the IoT device. 9. Ability to "sanitize" or "purge" specific or all data in the device.	Mandatory for Class 1 and above

Table-11: Device software Policies, and controls

DEVICE OPERATING SYSTEM

This section provides policies, controls and considerations required for securing the device's operating system. Including controls for system update, system accounts, passwords, system services, OS kernel, execution, resource usage, device integrity and device operations.

The following table lists these requirements and controls, it follows the IoTSF Security Assurance Framework selected requirements from 2.4.6.1 through 2.4.6.15 and the NIST SP800-53Ar5 selected requirements from SC-02 through SC-51, PE-10 through PE-15, CM-02 through CM-08, CP-10, CP-12, SI-06, SI-17, CA-09(1), SR-09, SR-09(1) and IR-04(5)

Req. No	Security Requirements	Security Class
DO-01	The OS is implemented with relevant security updates prior to release.	Mandatory for Class 2 and above

Req. No	Security Requirements	Security Class
DO-02	All unnecessary accounts or logins have been disabled or eliminated from the software at the end of the software development process, e.g., development or debug accounts and tools.	Mandatory for Class 1 and above
DO-03	Files, directories and persistent data are set to minimum access privileges required to correctly function.	Mandatory for Class 1 and above
DO-04	Security parameters and passwords should not be hard-coded into source code or stored in a local file. If passwords absolutely must be stored in a local file, then the password file(s) are owned by, and are only accessible to and writable by, the Device's OS most privileged account and are obfuscated.	Mandatory for Class 1 and above
DO-05	All OS non-essential services have been removed from the product's software, image or file systems.	Mandatory for Class 1 and above
DO-06	All OS command line access to the most privileged accounts has been removed from the OS	Mandatory for Class 1 and above
DO-07	All of the product's OS kernel and services or functions are disabled by default unless specifically required. Essential kernel, services or functions are prevented from being called by unauthorized external product level interfaces and applications.	Mandatory for Class 1 and above
DO-08	All software is operated at the least privilege level possible and only has access to the resources needed as controlled through appropriate access control mechanisms.	Mandatory for Class 1 and above
DO-09	All the applicable security features supported by the OS are enabled.	Mandatory for Class 1 and above
DO-10	The OS is separated from the application(s) and is only accessible via defined secure interfaces.	Mandatory for Class 1 and above
DO-11	The OS implements a separation architecture to separate trusted from untrusted applications.	Mandatory for Class 2 and above
DO-12	The product's OS kernel is designed such that each component runs with the least security privilege required (e.g. a microkernel architecture), and the minimum functionality needed. (2.4.6.6/8 requires non-essential components to be disabled or removed).	Mandatory for Class 2 and above.
DO-13	The Product OS should be reviewed for known security vulnerabilities particularly in the field of cryptography prior to each update and after release. Cryptographic algorithms, primitives, libraries and protocols should be updateable to address any vulnerabilities.	Mandatory for Class 1 and above
DO-14	The user interface is protected by an automatic session idle logout timeout function.	Mandatory for Class 1 and above
DO-15	Secure Execution: 1. Ability to enforce organizationally-defined execution policies. 2. Ability to execute code in confined virtual environments.	Mandatory for Class 2 and above

Req. No	Security Requirements	Security Class
	3. Ability to separate IoT device processes into separate execution domains. 4. Ability to separate the levels of IoT device user functionality. 5. Ability to authorize various levels of IoT device functionality.	
DO-16	Secure Resource Usage: 1. Ability to support shared system resources. 2. Ability to release resources back to the system. 3. Ability to separate user and process resources. 4. Ability to manage memory address space assigned to processes. 5. Ability to enforce access to memory space through the kernel. 6. Ability to prevent a process from accessing memory space of another process. 7. Ability to enforce configured disk quotas. 8. Ability to continue operation when associated networks are unavailable (e.g., a smart smoke detector must still go off when a fire occurs even if it is not attached to the associated network). 9. Ability to provide sufficient resources to store and run the operating environment (e.g., operating systems, firmware, applications). 10. Ability to utilize file compression technologies (e.g., to provide denial of service protection). 11. Ability to use or enforce hardware-based, write protection to protect certain software (e.g., firmware).	Mandatory for Class 1 and above
DO-17	Device Integrity: 1. Ability to perform security compliance checks on system components (e.g., verify acceptable baseline configuration, perform a tamper check). 2. Ability to detect unauthorized hardware and software components and other tampering with the IoT device when used. 3. Ability to detect tampering throughout the system development life cycle. 4. Ability to take organizationally-defined actions when unauthorized hardware and software components are detected (e.g., disallow a flash drive to be connected even if a USB port is present). 5. Ability to store the operating environment (e.g., firmware image, software, applications) in read-only media (e.g., Read Only Memory).	Mandatory for Class 2 and above
DO-18	Secure Device Operation: 1. Ability to keep an accurate internal system time. 2. Ability to compare and synchronize internal system time with an organizationally defined authoritative source. 3. Ability to define various operational states. 4. Ability to support various modes of IoT device operation with more restrictive operational states. 5. Ability to define differing failure types. 6. Ability to fail in a secure state. 7. Ability to disable operations and/or functionality in the event of security violations. 8. Ability to restrict components/features of the IoT device (e.g., ports, functions, protocols, services, etc.) in accordance with organizationally-defined policies.	Mandatory for Class 2 and above

Req. No	Security Requirements	Security Class

Table-12: Device OS Policies, and controls

DEVICE WIRED AND WIRELESS INTERFACES

This section provides policies, controls and considerations required for securing both wired and wireless interfaces of the device, which are used to communicate with the device through some network. It Includes controls for securing connection, network configuration, unauthorized changes, system ports, connection passwords, authentication, communication keys, relevant communication protocols, communication availability and confidentiality, critical operations and misconfiguration.

The following table lists these requirements and controls, it follows the IoTSF Security Assurance Framework requirements 2.4.7.1 through 2.4.7.25

Req. No	Security Requirements	Security Class
DW-01	The product prevents unauthorized connections to it or other devices the product is connected to.	Mandatory for Class 1 and above
DW-02	The network component and firewall (if applicable) configuration has been reviewed and documented for the required/defined secure behavior.	Mandatory for Class 1 and above
DW-03	To prevent bridging of security domains within products with network interfaces, forwarding functions should be blocked by default.	Mandatory for Class 1 and above

Req. No	Security Requirements	Security Class
DW-04	Devices support only the versions of application layer protocols that have been reviewed and evaluated against publicly known vulnerabilities.	Mandatory for Class 1 and above
DW-05	If a potential unauthorized change is detected (e.g.: an access fails authentication or integrity checks), the device should alert the user/administrator to the issue and should not connect to wider networks than those necessary to perform the alerting function. Failed attempts should be logged, but without providing any information about the failure to the initiator.	Mandatory for Class 1 and above
DW-06	All the product's unused ports (or interfaces) are closed and only the necessary ones are active.	Mandatory for Class 1 and above
DW-07	If a connection requires a password or passcode or passkey for connection authentication, the factory issued or reset password is unique to each device.	Mandatory for all classes
DW-08	Where using the initial pairing process, a Strong Authentication shall be used, requiring physical interaction with the device or possession of a shared secret.	Mandatory for Class 1 and above
DW-09	Where a wireless interface has an initial pairing process, the passkeys are changed from the factory issued, or reset password prior to providing normal service.	Mandatory for all classes
DW-10	For any Wi-Fi connection, WPA-2 AES or a similar strength encryption has been used. Migration to the latest standard should be planned. (e.g., WPA3) Older insecure protocols such as WEP, WPA/WPA2 (Auto), WPA-TKIP and WPA-2 TKIP/AES (Mixed Mode) are disabled.	Mandatory for Class 1 and above
DW-11	Where WPA-2 WPS is used it has a unique, random key per device and enforces exponentially increasing retry attempt delays.	Mandatory for Class 1 and above
DW-12	All network communications keys are stored securely, in accordance with industry standards.	Mandatory for Class 1 and above
DW-13	Where a TCP protocol, such as MQTT, is used, it is protected by a TLS connection with no known vulnerabilities.	Mandatory for Class 1 and above
DW-14	Where a UDP protocol is used, such as CoAP, it is protected by a DTLS connection with no known vulnerabilities.	Mandatory for Class 1 and above
DW-15	Where cryptographic suites are used such as TLS, all cipher suites shall be listed and validated against the current security recommendations such as NIST 800-131A or OWASP. Where insecure ciphers suites are identified they shall be removed from the product.	Mandatory for Class 1 and above
DW-16	All use of cryptography by the product, such as TLS cipher suites, shall be listed and validated against the import/export requirements for the territories where the product is to be sold and/or shipped.	Mandatory for Class 1 and above
DW-17	Where there is a loss of communications or availability it shall not compromise the local integrity of the device.	Mandatory for Class 1 and above

Req. No	Security Requirements	Security Class
DW-18	The product only initializes and enables the communications interfaces, network protocols, application protocols and network services necessary for the product's operation.	Mandatory for Class 1 and above
DW-19	Communications protocols should be the latest versions with no publicly known vulnerabilities and/or appropriate for the product.	Mandatory for Class 1 and above
DW-20	Post product launch, communications protocols should be reviewed throughout the product life cycle against publicly known vulnerabilities and changed to the most secure versions available if appropriate.	Mandatory for Class 1 and above
DW-21	If a factory reset is made, the device should warn that secure operation may be compromised until updated.	Mandatory for Class 1 and above
DW-22	Where RF communications are enabled (e.g., ZigBee, etc.) antenna power is configured to limit the ability of mapping assets to limit attacks such as WAR-Driving.	Advisory for all classes
DW-23	Protocol anonymity features are enabled in protocols (e.g., Bluetooth) to limit location tracking capabilities.	Advisory for all classes
DW-24	As far as reasonably possible, devices should remain operating and locally functional in the case of a loss of network connection.	Mandatory for Class 1 and above
DW-25	Following restoration of power or network connection, devices should be able to return to a network in a sensible state and in an orderly fashion, rather than in a massive scale reconnect, which collectively could overwhelm a network.	Mandatory for Class 1 and above

Table-13: Device wireless and wired interfaces security Policies, and controls

AUTHENTICATION AND AUTHORIZATION

This section provides policies, controls and considerations for system authentication and authorization security. It includes controls for mitigating tampering, impersonation, creating weak passwords, brute force repeated login attempts, unauthorized access and securing passwords creation, passwords storing, password recovery and reset, passwords entry and device authentication and identification.

The following table lists these requirements and controls, it follows the IoTSF Security Assurance Framework requirements 2.4.8.1 through 2.4.8.18 and the NIST SP800-53Ar5 selected requirements from IA-02 through IA-06 and AC-17(10)

Req. No	Security Requirements	Security Class
AA-01	The product contains a unique and tamper-resistant device identifier. E.g., the chip serial number or other unique silicon identifier, for example to bind code and data to a specific device hardware. This is to mitigate threats from cloning and also to ensure authentication may be done assuredly using the device identifier e.g., using a device certificate containing the device identifier.	Mandatory for all classes
AA-02	Where the product has a secure source of time there is a method of validating its integrity.	Mandatory for Class 1 and above
AA-03	Where a user interface password is used for login authentication, the factory issued or reset password is randomly unique for every device in the product family. If a password-less authentication is used the same principles of uniqueness apply.	Mandatory for all classes
AA-04	The product does not accept the use of null or blank passwords.	Mandatory for all classes
AA-05	The product will not allow new passwords containing the user account name with which the user account is associated.	Mandatory for all classes
AA-06	Password entry follows industry standard practice on password length, characters from the groupings and special characters.	Mandatory for all classes
AA-07	The product has defense against brute force repeated login attempts, such as exponentially increasing retry attempt delays.	Mandatory for Class 1 and above
AA-08	The product securely stores any passwords using an industry standard cryptographic algorithm, compliant with an industry standard.	Mandatory for Class 1 and above
AA-09	The product supports access control measures to the root/highest privilege account to restrict access to sensitive information or system processes.	Mandatory for Class 1 and above
AA-10	The access control privileges are defined, justified and documented.	Mandatory for Class 1 and above
AA-11	The product only allows controlled user account access; access using anonymous or guest user accounts is not supported without justification.	Mandatory for Class 1 and above
AA-12	The product allows the factory issued or OEM login accounts to be disabled or erased or renamed when installed or commissioned.	Advisory for all classes
AA-13	The product supports having any or all of the factory default user login passwords altered when installed or commissioned.	Mandatory for all classes
AA-14	If the product has a password recovery or reset mechanism, an assessment has been made to confirm that this mechanism cannot readily be abused by an unauthorized party.	Mandatory for Class 1 and above

Req. No	Security Requirements	Security Class
AA-15	Where passwords are entered on a user interface, the actual pass phrase is obscured by default.	Mandatory for Class 1 and above
AA-16	The product allows an authorized and complete factory reset of all of the device's authorization information.	Advisory for all classes
AA-17	Where the product has the ability to remotely recover from attack, it should rely on a known good state, to enable safe recovery and updating of the device, but should limit access to sensitive assets until the device is in a known secure condition.	Mandatory for Class 1 and above
AA-18	Devices are provided with a RoT-backed unique authenticable logical identity.	Mandatory for Class 1 and above
AA-19	Device Authentication Support: 1. Ability for the IoT device to identify itself as an authorized entity to other devices. 2. Ability to verify the identity of other devices.	Mandatory for Class 1 and above
AA-20	Authentication Support: 1. Ability for the IoT device to require authentication prior to connecting to the device, including using remote access. 2. Ability for the IoT device to support and require appropriate authentication. 3. Ability for the IoT device to support a second, or more, authentication method(s) through an out of band path such as: Temporary passwords or other one-use logon credentials, Third-party credential checks, Biometrics, Text messages, other methods 4. Ability for the IoT device to hide or mask authentication information during the authentication process.	Mandatory for Class 1 and above

Table-14: Device Authentication and Authorization Policies, and controls.

ENCRYPTION AND KEY MANAGEMENT FOR HARDWARE

This section provides policies, controls and considerations for encryption and key management security. It includes controls for securing security parameters, keys confidentiality, cryptographic functions, sensitive parameters storing, private keys, cryptographic capabilities and key management, data transmission and security and privacy attributes transmission.

The following table lists these requirements and controls, it follows the IoTSF Security Assurance Framework requirements 2.4.9.2 through 2.4.9.11 and the NIST SP800-53Ar5 selected requirements from SC-02 through SC-28 and SA-9(6)

Req. No	Security Requirements	Security Class
EK-01	If present, a true random number generator source has been validated for true randomness.	Mandatory for Class 2 and above
EK-02	There is a process for secure provisioning of security parameters and keys that includes random and individual (unique) generation, distribution, update, revocation and destruction.	Mandatory for Class 2 and above
EK-03	There is a secure method of key insertion that protects keys against copying.	Mandatory for Class 1 and above
EK-04	All the product related cryptographic functions have no publicly known unmitigated weaknesses in the algorithms or implementation, for example MD5, SHA-1, and DES are not used.	Mandatory for Class 1 and above
EK-05	All the product related cryptographic functions are sufficiently secure for the lifecycle of the product, or cryptographic algorithms and primitives should be updateable ("crypto agility").	Mandatory for Class 1 and above
EK-06	The product stores all sensitive unencrypted parameters (e.g., keys) in a secure, tamper-resistant location.	Mandatory for Class 1 and above
EK-07	The cryptographic key chain used for signing production software is different from that used for any other test, development or other software images or support requirement.	Advisory for all classes
EK-08	In device manufacture, all asymmetric encryption private keys that are unique to each device are secured. They must be truly randomly internally generated or securely programmed into each device.	Mandatory for Class 2 and above
EK-09	All key lengths are sufficient for the level of assurance required.	Mandatory for Class 2 and above
EK-10	In systems with many layered sub devices, key management should follow best practice.	Mandatory for all classes
EK-11	Cryptography Capabilities and Support: 1. Ability to execute cryptographic mechanisms of appropriate strength and performance. 2. Ability to obtain and validate certificates. 3. Ability to verify digital signatures. 4. Ability to run hashing algorithms (i.e., compute and compare hashes). 5. Ability to perform authenticated encryption algorithms.	Mandatory for Class 2 and above
EK-12	Cryptographic Key Management: 2. Ability to manage cryptographic keys securely 3. Ability to generate key pairs. 4. Ability to store encryption keys securely. 5. Ability to change keys securely. 6. Ability to maintain exclusive control of cryptographic keys when used by external systems.	Mandatory for Class 2 and above
EK-13	Secure Transmission: 1. Ability to configure the cryptographic algorithm to protect data in transit.	Mandatory for all classes

Req. No	Security Requirements	Security Class
	2. Ability to support trusted data exchange with a specified minimum strength cryptography algorithm. 3. Ability to support data encryption and signing to prevent data from being altered in transit. 4. Ability to utilize one or more capabilities to protect the data it transmits from unauthorized access and modification. 5. Ability to use cryptographic means to validate the integrity of data transmitted. 6. Ability to use organization-internal normalized formats to protect the data it transmits.	
EK-14	SEPARATION OF SYSTEM AND USER FUNCTIONALITY: 1. user functionality, including user interface services, is separated from system management functionality 2. state information is stored separately from applications and software	Mandatory for Class 2 and above
EK-15	TRANSMISSION OF SECURITY AND PRIVACY ATTRIBUTES: 1. the integrity of transmitted security attributes is verified 2. the integrity of transmitted privacy attributes is verified. 3. anti-spoofing mechanisms are implemented to prevent adversaries from falsifying the security attributes indicating the successful application of the security process	Mandatory for Class 1 and above
EK-16	Information at rest requiring protection is defined;	Mandatory for Class 1 and above

Table-15: Encryption and key management security Policies, and controls

CYBERSECURITY STATE AWARENESS

This section provides policies, controls and considerations for cybersecurity state awareness, it is required to add ability to get information about the cybersecurity state of the IoT device. It includes controls for getting access to events information, identification, monitoring and response.

The following table lists these requirements and controls, it follows the NIST SP800-53Ar5 selected requirements from AU-02 through AU-13, SC-07 through SC-42, SI-04, CM-03, CM-06, CA-07, IA-02, CP-13, IR-04 and RA-07.

Req. No	Security Requirements	Security Class
CS-01	Access to Event Information: 1. Ability to access information about the IoT device's cybersecurity state and other necessary data.	Mandatory for all classes

Req. No	Security Requirements	Security Class
	2. Ability to preserve system state information.	
CS-02	Event Identification & Monitoring: 1. Ability to identify organizationally-defined cybersecurity events (e.g., expected state change) that may occur on or involving the IoT device. 2. Ability to monitor for organizationally-defined cybersecurity events (e.g., expected state change) that may occur on or involving the IoT device. 3. Ability to support a list of events that are necessary for auditing purposes (to support the organizational auditing policy). 4. Ability to identify unique users interacting with the device (to allow for user session monitoring). 5. Ability to support a monitoring process to check for disclosure of organizational information to unauthorized entities. (The device may be able to perform this check itself or provide the information necessary for an external process to check) 6. Ability to monitor communications traffic. 7. Ability to monitor changes to the configuration settings. 8. Ability to detect remote activation attempts. 9. Ability to define the characteristics of unapproved content. 10. Ability to scan files for unapproved content.	Mandatory for all classes
CS-03	Event Response: 7. Ability to generate alerts for specific events. 8. Ability to respond to alerts according to predefined responses. 9. Ability to alert connected information systems of potential issues found during the auditing process. 10. Ability to provide information to an external process that will issue auditing process alerts. 11. Ability to notify users of activation of a collaborative computing device. 12. Ability to provide a physical indicator of sensor use. 13. Ability to respond following an auditing failure (either by the device or an external auditing process). 14. Ability to prevent download of unapproved content 15. Ability to delete unapproved content. 16. Ability to support alternative security mechanisms when primary mechanisms (e.g., login protocol, encryption, etc.) are compromised. 17. Ability to configure organizationally-defined aspects of the event response.	Mandatory for Class 2 and above

Table-16: Cybersecurity state awareness Policies, and controls

WEB USER INTERFACE

This section provides policies, controls and considerations for web user interface security. Including controls for securing management and login authentication, access roles, user passwords, password entry, data transfer, sessions, inputs and outputs, web interfaces and personal data communication.

The following table lists these requirements and controls, it follows the IoTSF Security Assurance Framework selected requirements from 2.4.10.1 through 2.4.10.19

Req. No	Security Requirements	Security Class
UI-01	Where the product or service provides a web-based user interface, Authentication is secured using current best practice cryptography.	Mandatory for Class 1 and above
UI-02	Where the product or service provides a web browser-based interface, access to any restricted/administrator area or functionality shall require authentication.	Mandatory for Class 1 and above
UI-03	Where the product or service provides a web-based management interface, Authentication is secured using current best practice cryptography.	Mandatory for Class 1 and above
UI-04	Where a web user interface password is used for login authentication, the initial password or factory reset password is unique for every device in the product family.	Mandatory for all classes
UI-05	The web user interface is protected by an automatic session idle logout timeout function.	Mandatory for Class 1 and above
UI-06	User passwords are not stored in plain text.	Mandatory for all classes
UI-07	Strong passwords are required, and a random salt value is incorporated with the password.	Mandatory for Class 1 and above
UI-08	Where passwords are entered on a user interface, the actual pass phrase is obscured by default to prevent the capture of passwords.	Mandatory for Class 1 and above
UI-09	The web user interface shall follow good practice guidelines.	Mandatory for Class 1 and above
UI-10	A vulnerability assessment has been performed before deployment and is repeated periodically throughout the lifecycle of the service or product.	Mandatory for Class 1 and above
UI-11	All data being transferred over interfaces should be validated where appropriate. This could include checking the data type, length, format, range, authenticity, origin and frequency.	Mandatory for Class 1 and above

Req. No	Security Requirements	Security Class
UI-12	Sanitize input in Web applications by using URL encoding or HTML encoding to wrap data and treat it as literal text rather than executable script.	Mandatory for Class 1 and above
UI-13	All inputs and outputs are validated using for example an allow list (formerly 'whitelist') containing authorized origins of data and valid attributes of such data.	Mandatory for Class 1 and above
UI-14	Administration Interfaces are accessible only by authorized operators. Mutual Authentication is used over administration interfaces, for example, by using certificates.	Mandatory for Class 1 and above
UI-15	Reduce the lifetime of sessions to mitigate the risk of session hijacking and replay attacks. (For example, to reduce the time an attacker has to capture a session cookie and use it to access an application).	Mandatory for Class 1 and above
UI-16	All inputs and outputs are checked for validity. Tests to include both expected (valid) and unexpected (invalid) input stimuli.	Mandatory for Class 1 and above
UI-17	Web Interfaces should be developed using best practice secure coding techniques and server frameworks.	Mandatory for Class 1 and above
UI-18	Password entry follows industry standard practice.	Mandatory for all classes
UI-19	Web interface should provide a simple method (one to two clicks) to initiate any security update to the end device.	Mandatory for all classes
UI-20	Any personal data communicated between the web interface and the device shall be encrypted. Where the data includes sensitive personal data then the encryption must be appropriately secure.	Mandatory for all classes

Table-17: Web UI Policies, and controls

MOBILE APPLICATION

This section provides policies, controls and considerations for securing mobile applications used with IoT solutions. It includes controls for securing user interface passwords, password entry, databases and files, connection to remote servers, passwords storage, data transfer, configuration management, inputs and outputs, application updates, network access and personal data communication.

The following table lists these requirements and controls, it follows the IoTSF Security Assurance Framework requirements 2.4.11.1 through 2.4.11.13

Req. No	Security Requirements	Security Class
MA-01	Where an application's user interface password is used for login authentication, the initial password or factory reset password is unique to each device in the product family.	Mandatory for all classes
MA-02	Password entry follows industry standard practice.	Mandatory for all classes
MA-03	The mobile application ensures that any related databases or files are either tamper resistant or restricted in their access. Upon detection of tampering of the databases or files, they are re-initialized.	Mandatory for Class 1 and above
MA-04	Where the application communicates with a product related remote server(s), or device, it does so over a secure connection.	Mandatory for Class 1 and above
MA-05	The product securely stores any passwords using an industry standard cryptographic algorithm.	Mandatory for Class 1 and above
MA-06	Where passwords are entered on a user interface, the actual pass phrase is obscured by default to prevent the capture of passwords.	Mandatory for Class 1 and above
MA-07	All data being transferred over interfaces should be validated where appropriate. This could include checking the data type, length, format, range, authenticity, origin and frequency.	Mandatory for Class 1 and above
MA-08	Secure Administration Interfaces; It is important that configuration management functionality is accessible only by authorized operators and administrators. Enforce Strong Authentication over administration interfaces, for example, by using certificates.	Mandatory for Class 1 and above
MA-09	All application inputs and outputs are validated using for example a allowed list containing authorized origins of data and valid attributes of such data.	Mandatory for Class 1 and above
MA-10	Mobile Apps should be developed using best practice secure coding techniques and server frameworks.	Mandatory for Class 1 and above
MA-11	App interface should provide a simple method (one to two clicks) to initiate any security update to the end device.	Mandatory for Class 1 and above
MA-12	Access to device functionality via a network/web browser interface in the initialized state should only be permitted after successful Authentication using current best practice secure cryptographic modules.	Mandatory for Class 1 and above
MA-13	Any personal data communicated between the mobile app and the device shall be encrypted. Where the data includes sensitive personal data then the encryption must be appropriately secure.	Mandatory for Class 1 and above

Table-18: Mobile application security Policies, and controls.

CLOUD AND NETWORK ELEMENTS

This section provides policies, controls and considerations for securing the cloud and network elements used by the IoT solution. It includes controls for securing operating system, web services, web services protocols, web servers, communication through the web, user passwords, passwords storage, unauthenticated access, service availability, cloud communication, device identity and configuration, user roles, API keys, related cloud services, cloud databases, remote access and personal data communication; and mitigating password brute force attacks, DDOS attacks and malfunctioning or malicious activities.

The following table lists these requirements and controls, it follows the IoTSF Security Assurance Framework selected requirements from 2.4.13.1 through 2.4.13.36

Req. No	Security Requirements	Security Class
CN-01	All the product related cloud and network elements have the latest operating system(s) security updates implemented and processes are in place to keep them updated.	Mandatory for Class 2 and above
CN-02	Any product related web servers have their web server identification options (e.g., Apache or Linux) switched off.	Mandatory for Class 1 and above
CN-03	All product related web servers have their web server HTTP trace and trace methods disabled.	Mandatory for Class 1 and above
CN-04	All the product related web servers' TLS certificate(s) are signed by trusted certificate authorities; are within their validity period; and processes are in place for their renewal.	Mandatory for Class 1 and above
CN-05	The Product Manufacturer or Service Provider has a process to monitor the relevant security advisories to ensure all the product related web servers use protocols with no publicly known weaknesses.	Mandatory for Class 1 and above
CN-06	The product related web servers support appropriately secure TLS/DTLS ciphers and disable/remove support for deprecated ciphers.	Advisory for all classes
CN-07	The product related web servers have repeated renegotiation of TLS connections disabled.	Mandatory for Class 1 and above
CN-08	The related servers have unused IP ports disabled.	Mandatory for Class 1 and above
CN-09	Where a product related to a web server encrypted communications using TLS and requests a client certificate, the server(s) only establishes a connection if the client certificate and its chain of trust are valid.	Mandatory for Class 1 and above

Req. No	Security Requirements	Security Class
CN-10	Where a product related to a web server encrypted communications using TLS, certificate pinning is implemented.	Advisory for all classes
CN-11	All the related servers and network elements prevent the use of null or blank passwords.	Mandatory for Class 1 and above
CN-12	All the related servers and network elements enforce passwords that follow industry good practice.	Mandatory for Class 1 and above
CN-13	Brute force attacks are impeded by introducing escalating delays following failed user account login attempts, and/or a maximum permissible number of consecutive failed attempts.	Mandatory for Class 1 and above
CN-14	All the related servers and network elements store any passwords using a cryptographic implementation using industry standard cryptographic algorithms.	Mandatory for Class 1 and above
CN-15	All the related servers and network elements support access control measures to restrict access to sensitive information or system processes to privileged accounts.	Mandatory for Class 1 and above
CN-16	All the related servers and network elements prevent anonymous/guest access except for read only access to public information.	Mandatory for Class 1 and above
CN-17	If run as a cloud service, the service meets industry standard cloud security principles.	Advisory for all classes
CN-18	Where a Product or Services includes any safety critical or life-impacting functionality, the services infrastructure shall incorporate protection against DDOS attacks, such as dropping of traffic or sink-holing.	Mandatory for Class 2 and above
CN-19	Where a Product or Service includes any safety critical or life-impacting functionality, the services infrastructure shall incorporate redundancy to ensure service continuity and availability.	Mandatory for Class 1 and above
CN-20	Input data validation should be maintained in accordance with industry best practice methods.	Mandatory for Class 1 and above
CN-21	If run as a cloud service, the cloud service TCP based communications (such as MQTT connections) are encrypted and authenticated using the latest TLS standard.	Mandatory for Class 1 and above
CN-22	If run as a cloud service, UDP-based communications are encrypted using the latest Datagram Transport Layer Security (DTLS).	Mandatory for Class 1 and above
CN-23	Where device identity and/or configuration registries (e.g., "thing shadows") are implemented to "on-board" devices within a cloud service, the registries are configured to restrict access to only authorized administrators.	Mandatory for Class 1 and above
CN-24	Product-related cloud services bind API keys to specific IoT applications and are not installed on non-authorized devices.	Mandatory for Class 2 and above

Req. No	Security Requirements	Security Class
CN-25	Product-related cloud services API keys are not hard-coded into devices or applications.	Mandatory for all classes
CN-26	If run as a cloud service, privileged roles are defined and implemented for any gateway/service that can configure devices.	Mandatory for Class 2 and above
CN-27	Product-related cloud service databases are encrypted during storage.	Mandatory for Class 1 and above
CN-28	Product-related cloud service databases restrict read/write access to only authorized individuals, devices and services.	Mandatory for Class 1 and above
CN-29	Product-related cloud services are designed using a defense-in-depth architecture consisting of Virtual Private Clouds (VPCs), firewalled access, and cloud-based monitoring.	Mandatory for Class 1 and above
CN-30	When implemented as a cloud service, all remote access to cloud services is via secure means (e.g., SSH).	Mandatory for Class 1 and above
CN-31	Product-related cloud services monitor for compliance with connection policies and report out-of-compliance connection attempts.	Mandatory for Class 2 and above
CN-32	IoT edge devices should connect to cloud services using secure hardware and services (e.g., TLS using private keys stored in secure hardware).	Mandatory for Class 1 and above
CN-33	Any personal data communicated between the mobile app and the device shall be encrypted. Where the data includes sensitive personal data then the encryption must be appropriately secure.	Mandatory for Class 2 and above
CN-34	Subject to user permission, telemetry data from the device should be analyzed for anomalous behavior to detect malfunctioning or malicious activity.	Mandatory for Class 2 and above

Table-19: Cloud and Network elements security Policies, and controls.

CONTINUOUS ASSESSMENT AND MONITOR

This section provides policies, controls and considerations for continuous assessments and monitoring of the IoT solution. It includes controls for developing assessment plans, gaining cyber security certifications, regular assessment and penetration testing and monitoring cyber security status of the IoT solution.

The following table lists these requirements and controls, it follows the NIST SP800-53Ar5 selected requirements from CA-02 through CA-08, CM-08, MA-03

Req. No	Security Requirements	Security Class
AM-01	Develop a control assessment plan that describes the scope of the assessment including: 1. Controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities;	Mandatory for Class 2 and above
AM-02	The IoT service provider and the provided IoT service/devices (can be hardware, firmware, cloud...etc.) must pass at least one cyber security certifications process matching the service domain. E.g., hardware can be certified from common criteria or PSA, sensitive software/firmware can be certified from common criteria.	Mandatory for Class 3 and above
AM-03	1) Conduct regular penetration testing on the provided services. 2) The frequency and the scope of the penetration testing process must be defined.	Mandatory for Class 2 and above
AM-04	1. The service's cyber security status and privacy status must be monitored in real time. 2. Any new discovered vulnerabilities need to be patched. 3. Vulnerabilities in 3rd party software/firmware must be patched.	Mandatory for Class 2 and above
AM-05	1) All the service components must receive regular software, firmware, and hardware updates. 2) The frequency of the updates must be defined. 3) The libraries and other 3rd party software/firmware components must be updated regularly to the latest versions.	Mandatory for all classes

Table-20: Continuous assessment and monitor Policies, and controls.

CONFORMITY ASSESSMENT

OVERVIEW

Conformity assessment is the final step of the IoT security assurance process, where conformity with the relevant security requirements is assessed with evidence. Figure-8 presents an overview of steps to complete the conformity assessment procedure, sequential steps and expected outcomes to perform this activity are provided in figure-5.

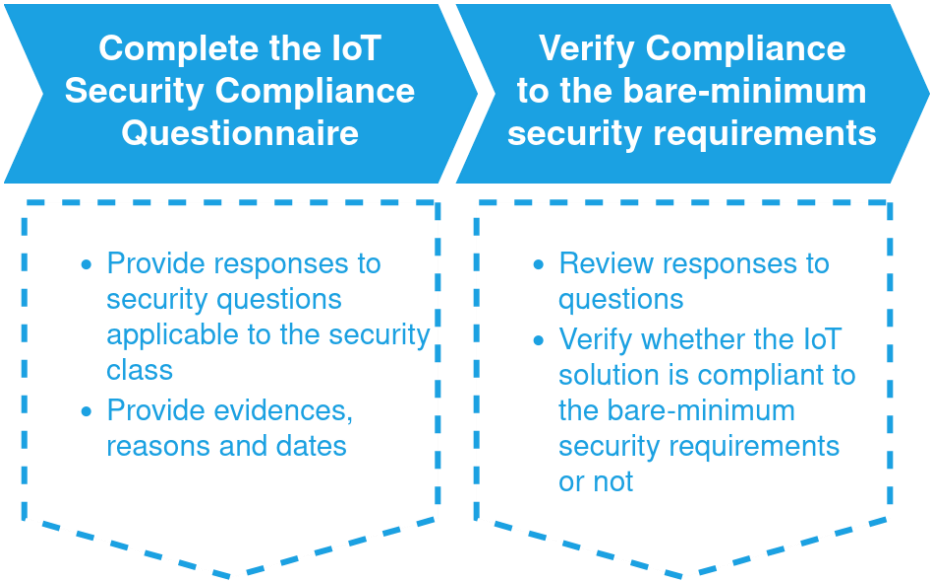


Figure-8: Conformity assessment procedure.

To do so, an IoT security compliance assessment questionnaire checklist covering the key requirements-based questions is provided, as an audit and assessment tool. Every requirement under questioning is accompanied with its corresponding applicable security classes. The organization shall answer questions of requirements covering the applicable security classes to determine the conformity of the service providing organization, and the IoT solution to the security guidelines.

Based on the outcomes of the risk assessment activity, the applicable security classes, for the solution of concern, are determined as discussed earlier in the process; then the applicable security requirements are automatically derived according to the corresponding

security class in the tool. And then, the organization is ready to go through answering the security compliance assessment questionnaire.

The organization shall answer all questions applicable on the determined security class of the IoT solution of concern. It should provide supporting evidence and reasons for their answers wherever possible. The resulting checklist answers should clearly verify whether the IoT solution of concern complies with the presented security baseline requirements or not. This compliance assessment questionnaire is intended to help organizations achieve high quality, informed security choices by guiding users through a robust checklist and evidence collecting process.

THE IOT SECURITY COMPLIANCE QUESTIONNAIRE

The IoT security compliance assessment questionnaire document is a part of the IoT Technical Security Guidelines in the ARE. It provides a security assessment questionnaire checklist to guide IoT service providing organizations through a security assessment process while collecting well-structured evidence and reasons, based on IoT security best practices and requirements. After completing this checklist, organizations should be able to determine the compliance level of the IoT solution of concern.

Few foundations have provided security compliance questionnaires and checklists for the IoT and cyber security in general. The IoT security compliance assessment questionnaire provided with this security assurance process follows applicable requirements from the IoT Security Compliance Framework provided by IoTSF (Internet of Things Security Foundation) and from the NIST SP800-53Ar5, where both are considered reliable and solid frameworks for relevant guidelines and standards.

The IoT security compliance assessment questionnaire can be found in Appendix-C. It is also available in a separate document as an editable sheet for interested organizations, which should facilitate the process of completing the questionnaire by adding answers directly in the sheet.

The editable sheet is attached to the document and available upon request.

This assessment questionnaire is intended to help organizations achieve high quality, informed security choices by guiding them through a robust checklist and evidence collecting process.

USING THE ASSESSMENT QUESTIONNAIRE

The process is guided by the category of the IoT solution under investigation and the corresponding applicable security class. In order to use this checklist questionnaire, the organization should first consider the IoT Security assurance process.

A risk assessment process should be first conducted in order to find applicable risk levels and factors, that is used to determine the precise impact for each security objective, confidentiality, integrity and availability levels (CIA-Triad); then consequently determine the corresponding security class for each, thus determining applicable security controls and requirements. For the detailed process and extra demonstration, please refer to the IoT Security assurance process.

COMPLIANCE CHECKLIST

The responsible organization's members shall answer each requirement by providing a response, evidence and a reason.

No	Mark	Response	Description
1	**C**	Compliant	The requirement is fully satisfied.
2	**PC**	Partially Compliant	The requirement is partially satisfied.
3	**NC**	Not Compliant	The requirement is not satisfied.
4	**N/A**	Not Applicable	The requirement is not applicable for the IoT solution of concern.

Table-21: Checklist response options.

Response: Response is selected from 4 options as shown and described in table-21.

Evidence: The response should be supplied by an evidence document ensuring the provided response, wherever possible.

Reason: A reason should be provided whenever needed to justify the provided response.

ASSESSMENT METHODOLOGY

The assessment method is affected by the context (here, technical) and the class. Together, they define the type of assessment, e.g., physical testing, software review or document review, along with the degree of firmness, from self-assessment for lower classes to full third-party audit for high classes.

After the service provider fills the questionnaire checklist document with the required input, an audit and review process are started by the NTRA to determine whether both the service providing organization and the provided technical service are compliant to the technical security guidelines or not. After audition and review, the NTRA then provides a security compliance assessment report with the resulting compliance level decision, along with recommendations and suggestions.

RESPONSIBILITIES & COMMITMENTS

- It is the responsibility of the service provider to provide accurate and realistic responses to the applicable security controls' questions. They must also provide relevant evidence, reasons and date of answering the question.
- The NTRA security committee is responsible for auditing responses of the compliance questionnaire and verifying whether answers are valid and accurate or not, and if accurate they are responsible for auditing whether the IoT solution is approved or rejected depending on the level of compliance to the IoT Security Compliance Questionnaire.
- The NTRA security committee has all the rights to request repeating any process on the condition that they detected any

means of providing misleading information or unrealistic evaluations through answers and outcomes generated by the service provider.

Responsibilities & commitments matrix summary

The following table (table-22) presents a summary of the security assurance process set of activities and the responsibility of each stakeholder through each one.

Activity	Entity responsible for performing the activity	Entity responsible for reviewing the activity and update if necessary	Entity responsible for auditing activity outcomes
Risk Assessment activity	Service Provider	Service Provider	NTRA Security Committee
Defining High Level Controls	Service Provider	Service Provider	NTRA Security Committee
Conformity Assessment	Service Provider	Service Provider	NTRA Security Committee
Commitments	This entity is committed to provide genuine and realistic information	This entity is committed to perform realistic review of provided information	This entity is committed to audit and validate outcomes of all activities and has all the rights to request repeating any activity of step of activity in case of detecting any imperfect, unrealistic or misleading data or information within outcomes

Table-22: A summary of the security assurance process activities with responsibilities and commitments of stakeholders

LIST OF TABLES AND FIGURES

LIST OF TABLES

LIST OF FIGURES

REFERENCES

- European Telecommunications Standards Institute (ETSI) EN 303 645 V2.1.1 (2020-06) - Cyber Security for Consumer Internet of Things: Baseline Requirements - https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
- UK Code of Practice for Consumer IoT Security - 2018 - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf
- Datta Burton, S.., Tanczer, L.M., Vasudevan, S., Hailes, S., Carr, M. (2021). The UK Code of Practice for Consumer IoT Security: 'where we are and what next'. The PETRAS National Centre of Excellence for IoT Systems Cybersecurity. DOI: 10.14324/000.rp.10117734 - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/978692/The_UK_code_of_practice_for_consumer_IoT_security_-_PETRAS_UCL_research_report.pdf
- IoTSF IoT Security Assurance Framework - Release-3.0-Nov-2021-1.
- IoT Cybersecurity: Regulation Ready - Full Version - Nov 2018 https://www.iotsecurityfoundation.org/wp-content/uploads/2018/11/IoT-Cybersecurity-Regulation-Ready-White-Paper-Full-Version.pdf
- Secure Design Best Practice Guides - Nov 2019 https://www.iotsecurityfoundation.org/wp-content/uploads/2019/12/Best-Practice-Guides-Release-2_Digitalv3.pdf
- GSMA IoT Security Guidelines - Overview Document - Version 2.2 - 29 February 2020 https://www.gsma.com/iot/wp-content/uploads/2020/05/CLP.11-v2.2-GSMA-IoT-Security-Guidelines-Overview-Document.pdf
- The OWASP IoT Attack Surface Areas - https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#IoT_Attack_Surface_Areas
- The OWASP IoT Top Ten - Internet of things 2018
- CISA Internet of Things Acquisition Guidance
- The NIST Framework for Improving Critical Infrastructure Cybersecurity - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- The NIST Special Publication 800-30r1 Guide for Conducting Risk Assessments - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
- The NIST Special Publication 800-53Ar5 - Assessing Security and Privacy Controls in Information Systems and Organizations - https://doi.org/10.6028/NIST.SP.800-53r5

- IoT Device Security Standards & Code of Practice for IoT Security - https://www.coderus.com/iot-device-security-standards-and-code-of-practice-for-iot-security/
- Anand, P.; Singh, Y.; Selwal, A.; Singh, P.K.; Felseghi, R.A.; Raboaca, M.S. IoVT: Internet of Vulnerable Things? Threat Architecture, Attack Surfaces, and Vulnerabilities in Internet of Things and Its Applications towards Smart Grids. *Energies* 2020, *13*, 4813. https://doi.org/10.3390/en13184813

APPENDIX-A: CASE STUDY

This section is intended to show how to use these guidelines to secure the IoT service provided by the service provider. It explains the complete step by step process to determine the compliance of an IoT service, and service provider to the technical security guidelines.

Consider a practical example of a smart grid service provider who offers an IoT connected smart electricity meter to the customers. The smart meters communicate to the AMI backend system to automatically send the readings and receive the commands from the service provider. The network keeps personal information about the clients since every meter is logically mapped to a specific client at a specific location, and the network collects information about the electricity consumption of the clients. These data are stored on the data centers of the service provider for further procession. The following process explained in figure-A-1 is needed to comply with the guidelines.

Figure-A-1: The Cybersecurity Process for the IoT technical security guidelines for the case study

1. Risk Assessment

1.1. Use case identification

The first step is defining the use cases of the provided service. The use cases have to be end-to-end use cases since it would be used later to determine the probable attack surfaces. The output is a list including all the possible use cases, functionalities, expected provided service. In this case study, a small sample for the use cases is created in table-A-1 as an explanation of the required output.

Use Case ID	Use Case	Functionality	Provided Service	System Components
01	Gathering readings from the smart meters	1. Smart meters to measure the power consumption. 2. Smart meters store the consumption values securely on the device till transmission. 3. Smart meters send the calculated readings to the AMI backend through LTE	Automatic readings submission to the service provider	Smart meter. LTE Communication modem. AMI Backend.
02	Executing commands from the service provider	1. Smart meters receive commands from the AMI backend based on the identity of every smart meter. 2. Smart meter is able to execute the command. 3. Smart meters report back the status to the AMI system.	Command execution based on the service provider requests.	Smart meter. LTE Communication modem. AMI Backend.

Table-A-1: Use case identification of the case study.

1.2. Attack surface areas & impact identification

For every use case, determine all the possible attack surfaces and the impacts on the system components and the provided service. A sample analysis in table-A-2 is provided to explain the required information in the output table.

Attack Surface	Vulnerabilities	Impact
Device Firmware	■ Sensitive data exposure (backdoor accounts, hardcoded credentials, encryption keys, sensitive information). ■ Firmware version display and/or last update date. ■ Vulnerable services (web, ssh, tftp, etc.). ■ Security related function API exposure. ■ Firmware downgrade possibility.	Injecting backdoor account on the smart meter can lead to sending incorrect readings and data to the service provider which leads to: - Taking wrong decisions based on false data - Financial loss to the service provider - Opening the door for more attacks on the device and network

Attack Surface	Vulnerabilities	Impact
Device Memory	▪ Sensitive data (Cleartext usernames, cleartext passwords, encryption keys).	Getting access to the combination encryption keys and parameters reveals the network data. This results in a huge information leak including personal information of the customers.
Privacy	▪ User data disclosure ▪ User/device location disclosure ▪ Differential privacy	Leaking personal user information such as identity, address, and consumption leads to privacy violations.
Vendor Backend APIs	▪ Inherent trust of cloud or mobile application ▪ Weak authentication ▪ Weak access controls ▪ Injection attacks ▪ Hidden services	Weak access controls lead to injection attacks and account takeover attacks. This may lead to taking control over the meters in a specific area or a complete denial of service.
Authentication/ Authorization	▪ Authentication/Authorization related values (session key, token, cookie, etc.) disclosure ▪ Reusing of session key, token, etc. ▪ Device to device authentication ▪ Device to mobile Application authentication ▪ Device to cloud system authentication ▪ Mobile application to cloud system authentication ▪ Web application to cloud system authentication ▪ Lack of dynamic authentication	Weak authentication between the meter and backend leads to rogue device attacks. This can lead to complete denial of service or taking control over the smart grid.
Update Mechanism	▪ Update sent without encryption ▪ Updates not signed ▪ Update location writable ▪ Update verification ▪ Update authentication ▪ Malicious update ▪ Missing update mechanism ▪ No manual update mechanism	Rogue updates sent to the smart grid network resulting in taking control over the whole smart meters network. May lead to catastrophic results such as power outage and faults in load balance.
Device Physical Interfaces	▪ Firmware extraction. ▪ User CLI. ▪ Admin CLI. ▪ Privilege escalation. ▪ Reset to an insecure state. ▪ Removal of storage media. ▪ Tamper resistance. ▪ Debug port (UART (Serial), JTAG / SWD). ▪ Device ID/Serial number exposure.	Ability to access the device may lead to modifying sensitive data such as encryption parameters, and tariff. This leads to financial loss for the service provider.

Table-A-2: Attack surface identification of the case study, with relevant vulnerabilities and its impact

1.3. Risk Analysis and Evaluation:

Using the reference risk assessment matrix in table-A-3 determine the overall risk for the exploitation of the attack surfaces depending on the likelihood and the impact level.

			Impact Level				
			Very Low	Low	Moderate	High	Very High
			Negligible effect	Limited effect	Serious effect	Severe effect	Multiple severe effects
Likelihood	Very High	Almost certain	Very Low	Low	Moderate	High	Very High
	High	Highly likely	Very Low	Low	Moderate	High	Very High
	Moderate	Somewhat likely	Very Low	Low	Moderate	Moderate	High
	Low	Unlikely	Very Low	Low	Low	Low	Moderate
	Very Low	Highly unlikely	Very Low	Very Low	Very Low	Low	Low

Table-A-3: Risk assessment matrix of the case study

Then map the likelihood and impact to table-A-4 to get the overall risk of every attack.

Risk level	Risk score	Description
Very Low	**[0-4]**	**Threat could be expected to have a negligible effect.**
Low	**[5-20]**	**Threat could be expected to have a limited effect.**
Moderate	**[21-79]**	**Threat could be expected to have a serious effect.**
High	**[80-95]**	**Threat could be expected to have a severe or catastrophic effect.**
Very High	**[95-100]**	**Threat could be expected to have multiple severe or catastrophic effects.**

Table-A-4: Risk levels and scores for risk assessment matrix of the case study

As a practical example, there is a very high probability that a hacker would tamper with the physical interface of the meter, and try to hack the physical interfaces such as UART, communication buses,etc.. In addition, the impact of such an attack is very high since it leads to multiple catastrophic effects on the network as explained in the attack surface identification in table-A-2. This means that the overall risk from such an attack is considered “very high” and has a score of “95-100”.

1.4. Findings documentation [Risk register]

Results are documented in a risk register document. A sample for the risk register is provided in table-A-5 for the smart meter use case.

Threat Description	Probability (0-100%)	Impact/Cost to company of threat happening (0-5)	Risk Factor
Tampering the physical interface and taking control over the smart meter	95%	5	**(0.95*5) = 4.75**
Exploiting update mechanism	10%	4	**(0.1*4) =0.4**
Breaking Authentication Mechanisms	10%	4	**(0.1*4) = 0.4**

Table-A-5: risk register for the case study.

1.5. Risk analysis review & update

Finally, the risk scores, impacts, and likelihood is reviewed to check if any additional modifications are needed before finishing documenting the findings to a risk register document.

2. High Level Security Requirements

The process of the high-level security requirements is intended to select the appropriate security class for the provided service which matches the impact and size of the threats and risks on the provided service. The process is explained in figure-A-2.

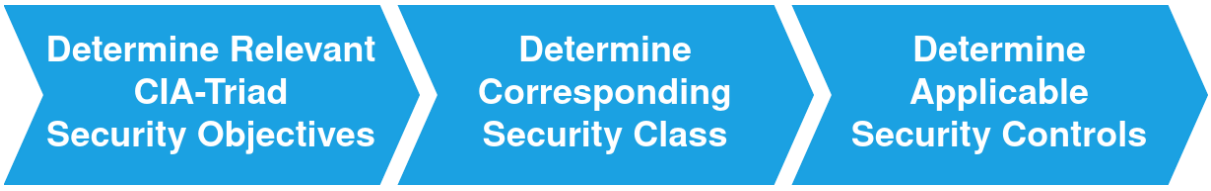


Figure-A-2: High level security requirements identification process.

2.1. Determine CIA Objectives

Based on the risk register document generated in the “Risk Assessment” process, the impact of the overall threats on confidentiality, integrity, and availability must be calculated according to table-A-6.

Object	Low Impact	Moderate Impact	High Impact
Confidentiality	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Table-A-6: CIA Objective

As a practical example for the smart meter case study, the risk register table-A-7 shows a very high impact and likelihood for the physical tampering threat. The impact of this threat can be mapped to the CIA as follows:

Confidentiality	Integrity	Availability
High impact Leaking sensitive information about the customers from the service provider database, and leaking credentials, are all considered catastrophic effects on the service provider and clients	**Moderate Impact** Unauthorized data modification may lead to serious damage to the service provider, e.g., unauthorized modification of the Tariff.	**High Impact** Any DoS attack can cause a complete power outage over a large geographical area, and may lead to faults in load balancing, explosions, and fires. These effects are considered catastrophic on service providers, clients, and the whole country.

Table-A-7: Impact of threat on the CIA objectives regarding the case study

2.2. Determine the Security Class

In this step, the output CIA impact is used to determine the correct security class for the provided service. In this case study, it is clear that the output is “Class 3” security requirements and controls.

2.3. Determine Applicable Security Class Controls

Finally, all controls and requirements marked as the following:

1. Mandatory for class 3 and above.
2. Mandatory for class 2 and above.
3. Mandatory for class 1 and above.
4. Mandatory for all classes.

are all mandatory requirements to be applied to the service providing organization, and the technical service, devices, and software provided to the customers.

3. Conformity Assessment

This is the final step in the process where the service provider answers all the questionnaires which determine the conformity of the service providing organization, and the technical service to the technical security guidelines. If the service provider, or the provided service is fully/partially compliant to the technical security guidelines, evidence must be provided to strengthen this claim. If the controls are not applicable for the service or the service is not compliant, a reason must be provided.

After the service provider fills the questionnaire document with the required input, the audit and review process from the NTRA starts to determine if both the service providing organization and the provided technical service are compliant to the technical security guidelines.

APPENDIX-B
IOT SECURITY COMPLIANCE ASSESSMENT QUESTIONNAIRE