1 Foreword

The fifth generation (**5G**) wireless technology represents a complete transformation of telecommunication networks. 5G will transform the digital landscape and serve as a catalyst for innovation, new markets, and economic growth. It is predicted that 5G networks will have more than 1.7 billion subscribers worldwide by 2025 [1].

Due to the increased bandwidth in the technology, this will enable new applications for the Internet of Things (**IoT**) and further accelerate the digital transformation. In fact, 5G will be critical towards the realisation of the Fourth Industrial Revolution (**4IR**) where billions of devices will be connected to the Internet through this technology. These connections will empower a vast array of new and enhanced critical infrastructure services. With IoT and 4IR, a plethora of new device types with less homogeneity than today's PCs and smartphones will relate to new and broader sets of applications. This is not just going to be internet-based applications and content, but rather real-time, mission-critical, and industrial control systems such as the Supervisory Control and Data Acquisition (**SCADA**). The next digital era will go beyond data behind screens and keyboards, but also enter the cyber physical domain through robots, sensors, and autonomous cyber physical processes.

The digital transformation will continue to introduce new dimensions of attack vectors, surfaces, and vulnerabilities through these connected digital systems. The IoT will bring a new set of issues, such as the security, safety, and robustness of the cyber-physical systems. Novel types of attack will bring new challenges to the industry by surprise. As such, more and more targets will be attractive and easy to approach by the cyber criminals.

Obviously, 5G marks the beginning of a new era, while it also brings in cybersecurity challenges to a successful 5G transformation. Thus, to overcome those challenges systematically and effectively under the situation of rapid ICT development, it is essential to design a 5G cybersecurity framework as a foundation to hold out. This framework should clarify different 5G cybersecurity areas, roles, and responsibilities. Then, based on the threats of OIC-CERT 5G cybersecurity risk repository and those from other sources, exact cybersecurity requirements to address 5G cybersecurity concerns can be determined. Consequently, the objective of this document is to design such a framework and provide the required 5G cybersecurity requirements. Considering the difference level of security capabilities among the member states, this framework and its security requirements would be designed as a baseline foundation, to provide guidance to OIC-CERT member states on regulating their 5G cybersecurity requirements, which can also be individually customised for the member states' specific requirements.

This OIC-CERT 5G framework is mainly intended for regulatory authorities of member states, with the purpose of assisting them in making policies on regulating 5G equipment vendors, mobile network operators (**MNO**s), and relevant service providers.

2 Introduction

As shown in the OIC-CERT 5G cybersecurity risk repository, the cybersecurity for 5G has been facing serious challenges in mitigating threats. These threats can raise various cybersecurity risks on the access network, transport network, core network, supply chain, operation & maintenance(**O&M**), and application services to name a few.

Undoubtedly, if there is no appropriate security approach being taken, those risks can then lead to invalid or incomplete applications, services, and network access. This will also involve data breaches which mainly surround the confidentiality of information in the networks and equipment, availability and integrity of the 5G based services, equipment and network functionality. Therefore, with the concern on the increasing cybersecurity threats and challenges, the understanding, mapping, and mitigating identified and upcoming threats in a well-designed, cost effective, and practical manner is essential.

It is crucial to systematically define a 5G cybersecurity architecture and security necessities, and to guide the OIC-CERT member states to build and improve 5G cybersecurity in a holistic way. Thus, it is indispensable to design an OIC-CERT 5G cybersecurity framework as a baseline foundation.

Firstly, this framework defines a layered 5G cybersecurity model to explicitly distinguish roles and responsibilities in securing 5G equipment, networks and applications, respectively. Then, for each layer, the corresponding baseline security requirements are given. Next, to ensure that those security requirements could be well and uniformly implemented by the OIC-CERT member states where the unified standard and certification are decided to be the foundation of this framework. In addition, trust must be based on verifiable facts, which should in turn be based on unified standards.

It is up to the actual stakeholders' requirements to apply or develop a standard or certification scheme. There are some standards and certification schemes that can be applied directly. Utilizing recognised standard and certification as references, this document would neither design any new standards and certification schemes, nor explain how to implement any references in the practice.

In this document:

i. **Section 2** specifically defines some terminology that are used for the following framework's description
ii. **Section 3** systematically introduces the OIC-CERT 5G cybersecurity framework, and
iii. **Section 4** defines a certification mechanism that will be useful in applying any possible certification.

3 Definitions

Table 1: Terminology Use in this Framework

Term	Description

Audit	A review and assessment that is implemented against the requirements previously set out
Audit Team	Collective group of auditors, generally to consist of two or more professional people, who are responsible for an audit job together
Audit Report	Document presenting the results of the audit conducted
Compliance Declaration	A written statement to demonstrate that the signatory can adhere to the previously assessed evidence to behave as expected by a particular requirement. Such declaration is provided to a security test laboratory for evaluation and assessment
Conformance Claim	A written statement that confirms the writer meets the targeted security requirements
Security Test Laboratory	A test laboratory that is ISO/IEC 17025 accredited in the context of OIC-CERT 5G network equipment security standard and that conducts network equipment evaluations. It can be owned by any entity
Evaluation	An assessment, carried out by a security test laboratory against the relevant defined Security Assurance Specification
Evaluation Report	A report produced by a security test laboratory to reflect the level of compliance of an evaluated thing according to a defined security assurance specification

4 OIC-CERT 5G Cybersecurity Framework

The objective of setting up the OIC-CERT 5G cybersecurity framework is to guide the members in developing, improving, and continuously managing their own 5G cybersecurity. For this purpose, the cybersecurity requirements are needed to prevent threats and to mitigate the raised risks that are described in the OIC-CERT 5G cybersecurity risk repository, and from other sources. Threats would involve access security, network domain security, user domain security, application domain security, service-based architecture (**SBA**) security and visibility and configurability of security.

It is unrealistic to build and maintain secure and resilient 5G networks, application services, and ensuring trustworthy network equipment through an all-in one solution. Referring to the communication protocols (OSI Seven layers and TCP/IP four layers), the telecommunication industry has been divided into a few layers, which cover network equipment, network, and application services. Accordingly, the OIC-CERT 5G cybersecurity framework concentrates on the security of equipment, network, and vertical application, which would be easy to distinguish roles and responsibilities of implement and deploy cybersecurity requirements.

In addition, for network equipment vendors, network operators, and application service providers, the security posture of each layer should consider the following factors:

- **Standard:** industry-led, recognised, and consensus-based cybersecurity standards are the best practice security requirements to guide cybersecurity development and improvement in an effective and appropriate manner. Following globally accepted standards can ensure that operations are cost-effective and sustainable for the entire 5G ecosystem. Besides, given a standard, it is also useful to guarantee the compliance by a certification scheme, which can also increase the trustworthiness of a certificated equipment, network, or service as a result.

- **Design & Implementation:** during this phase, since the standards define the requirement for building, improving, and maintaining a security posture, the vendor, operator, or service provider could also be guided to satisfy security requirement. This can be done when they develop mobile network equipment, deploy a mobile network, or provide an application service from the very beginning.
- **Configuration**: during development, operators should configure the network equipment and other components together to properly and securely make the network run in a particular network architecture. Secure network configurations is a significant challenge for operators, to do this, it is helpful to refer a well-recognised cybersecurity standard or best practice.
- **Operation**: even with well recognised standards, securely developed network equipment, and robust network configurations, the operators' and service providers' process and operations can still make significant impact on the overall network security posture. There is a need to do continuous risk assessment and mitigation during the operations.

Above all, because the standards can be a good guideline or requirements of developing and improving security, and certification could be a reliable tool to guarantee standard compliance. Unified standards and certification will be the foundation of this OIC-CERT 5G cybersecurity framework to normalize following deployment and implementation security requirements. With this, fragmentation and potentially conflicting cybersecurity requirements for OIC-CERT member states could be avoided. Certification gives stakeholders the confidence that a certified actor is exactly implementing targeted cybersecurity requirements as expected. This framework is shown by Figure 1.

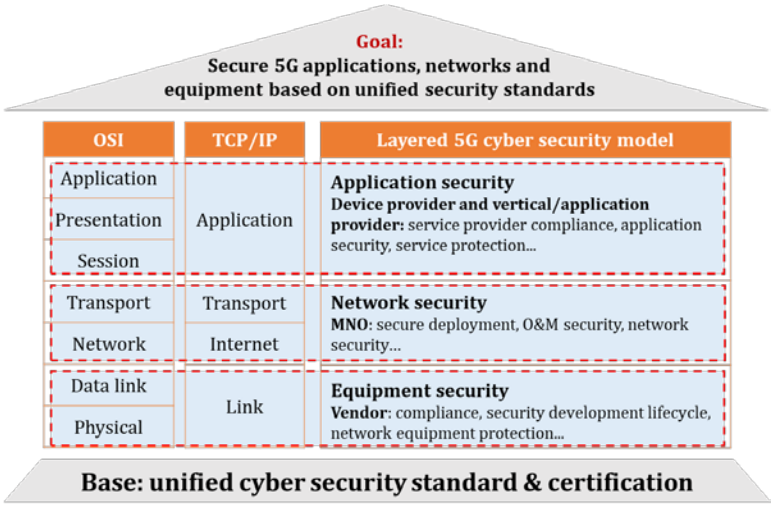

Figure 1 OIC-CERT 5G Cybersecurity Framework

Cybersecurity standards and certifications are only use as references. This is because applying or developing cybersecurity standards and certification schemes will depend on the requirements for the stakeholders. There are good standards and certifications for direct use. This document thereby focuses on guiding the design, application of standards and certifications according to security requirements. In line with this, for any selected references, it is not within the scope of this document to explain how to implement them into practice.

4.1 A Layered Security

Three (3) layers illustrated in Figure 1 is described below in detail.

4.1.1 Equipment Security Layer

Equipment security is the responsibility of the vendors who develop and maintain network equipment and supply them to the mobile network operators (**MNO**s). Network equipment security assurance is a key tool, which provides a basis to evaluate whether network equipment and components have been designed and operated in accordance with the proposed security requirements. Security assurance programmes should adhere to globally recognised and unified standards to ensure that their operation is cost effective, sustainable for the ecosystem, and security guaranteed.

The secure and robust network equipment provided by the vendors are necessary but not sufficient for the MNO. An equipment security assurance program can effectively help MNO to understand the level of security with a specific equipment provided by the vendor. According to this assurance result, the MNO can assess in advance whether their network security meets external regulation and oversight.

At the same time, in this document, the equipment security neither addresses the need for end-to-end 5G cybersecurity, nor involves security of interaction among the network equipment.

4.1.2 Network Security Layer

The network security layer is managed, controlled, and operated by the MNOs. During the network design and operation, MNOs perform comprehensive and continuous risk assessments. The operators need to consider network compliance and the security of the network design, deployment, operation and maintenance (**O&M**), and perform comprehensive and continuous risk assessment based on the network components, equipment provided by vendors, and network architectures.

4.1.3 Application Security Layer

This layer includes mobile device users and vertical industries that provide and use a range of applications. Application security requires a multi-party collaboration among the MNOs, mobile device suppliers, application developers, and service providers to ensure the security of the 5G devices, users, and services they support. An application security extends beyond the MNO, therefore, beyond their responsibilities.

Vertical industries must take responsibilities for the security of their solutions. They must introduce mechanisms to protect confidentiality, integrity, and availability on top of the built-in security controls offered by the MNOs, to further improve the overall security offerings.

4.2 Cybersecurity Requirements Related to Each Layer

After understanding the functions, roles, and responsibilities of implementing the 5G cybersecurity for the different layers, it is time to further figure out the corresponding

cybersecurity requirements for each layer. For easy and flexible implementation purposes, those following security requirements are specially designed as a baseline, to guide or assist with OIC-CERT members' 5G cybersecurity development. In this way, audiences can understand general security targets, and combine it with their own realities to customise the related 5G cybersecurity efficiently.

The requirements for developing, improving, and managing 5G cybersecurity are dynamic along with many other aspects, such as the security technologies, security mindset and awareness, laws and regulations, and current threat landscape. This means that an iterative update of the security requirement in the different stages is essential.

4.2.1 Equipment Security Requirements

It is imperative for the vendors to provide secure 5G network equipment that should also securely work when in use. This means that the equipment should be able to continuously fulfil the proposed security functionalities against threats while in operation. The equipment should also be secured throughout the entire development process. Therefore, the requirements should be for the entire equipment lifecycle, to prevent assets from being vulnerable against identified threats. Figure 2 represents the relationship of development and lifecycle, asset, threat, and security requirements.

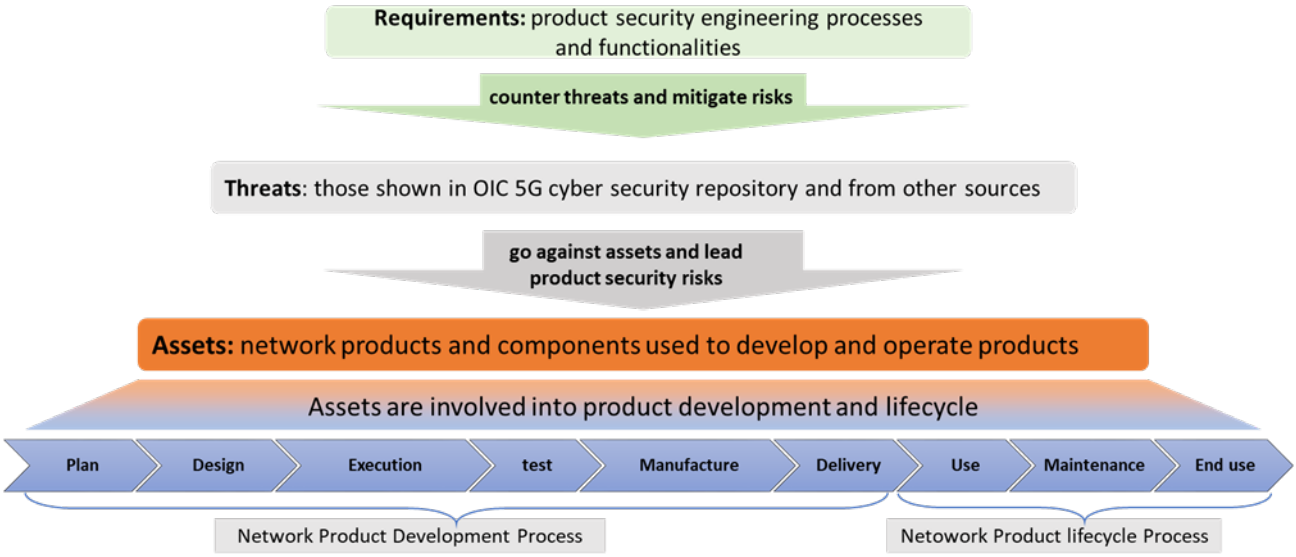

Figure 2 Equipment Security Requirement Overview

i. **Assets**: source code, software, hardware, manufactured equipment, operated equipment, security development files, development tools, systems, and environment

ii. **Threats**: raise security risks on network equipment, which could be breaching integrity and availability of equipment functions and components, which also be breaching the confidentiality of information within the equipment

The threats could be those illustrated in the OIC-CERT 5G Cybersecurity Risk Repository, including nefarious activities, abuse of assets, eavesdropping, interceptions, hijackings, physical attacks, unintentional damage, failures, and malfunctions. The threats can involve wrong documentation, vulnerability unawareness, sensitive message leak, and poor design from other sources.

iii. **Requirements**: focusing on the equipment development, lifecycle, and proposed security features and security requirements designed to counter threats and mitigate risks.

- Development security requirements will involve security & privacy by design, source code review, software integrity verification, development environment control, security test, staff training, and information security
- Lifecycle security requirements could contain version control, vulnerability management, staff training, third party management, improvements and optimizations
- Security functions requirement can be data protection, availability and integrity protection, authentication and authorization, secured session, and operating system security

iv. **References**: to better understand and implement equipment security requirements, it is essential to refer existing and well-recognised standards and practices. Two references are selected for this purpose:

- GSMA FS.16 Network Equipment Security Assurance Scheme- Development and Lifecycle Security Requirement v 2.0 [2]
- 3GPP TS 33.117 Catalogue of General Security Assurance Requirements [3]

4.3 Network security requirements

The 5G networks stake are facing increased value but decreased security risk tolerance. The networks performance security level is reliant on the deployment, operation, and maintenance of networks, which would be reflected by setting the security controls and strengthening the approaches. The network resilience is increasingly attracting attention from various stakeholders, such as the MNOs, governments and regulators.

Therefore, network security requirements would mainly focus on preventing threats and mitigating risks on both the network security and resilience. For security, the requirements will focus on preventing the system, data, and services from being damaged, tampered, or stolen. The resilience requirements will focus on timely recovery and high availability of systems, data, and services.

- **Threats**: in accordance with the OIC-CERT 5G Cybersecurity Risk Repository, threats against the networks can be classified as access network threats, core network threats, transport network threats, supply chain attacks, generic threats, and O&M threats. New technologies and functions (SBA/ NFV/ SDN/ MEC/ Slice) to the 5G networks may bring new challenges and threats.
- **Requirements**: based on the 5G network equipment security, various security devices are deployed to build the capabilities in the 5G security situational awareness, proactive security controls, security emergency handling, attack source tracing and recovery, and O&M security assurance, to make the security risks perceivable, visible, and controllable. Specifically, security and resilience requirements are classified into four high-level aspects:

i. *Security Risk Identification and Protection*: identify assets and implement asset-based risk discovery. Establish a 5G layer and domain based in-depth security protection system.

ii. *Monitoring and Handling*: monitor and detect the 5G network security attack events. Follow the unified response policies and interwork with various security protection devices and actors for automation response and alarming.

iii. *Recovery*: use the appropriate activities to maintain or recover any functions or services that are compromised due to the cybersecurity incidents.

iv. *Compliance*: comply with the laws, regulations, and regulatory requirements of the respective country.

- **References**: To better understand and implement the network security and resilience requirements, it is essential to refer to the existing and well-recognised standards and practices. References are selected but not limited to:

i. ISO/IEC 27001:2013 Information Security Management Systems (ISMS) [4]

ii. 3GPP Security Assurance Specifications (SCAS) TS 33. 514~522 [5]

iii. NIST Cyber Security Framework [6]

4.3.1 Application security requirements

Application security involves both traditional mobile end users and new vertical industries that provide or use a range of applications. It also involves device suppliers and application providers to ensure the security of the users and services they support. Application security is not heavily dependent on the security of network. Vertical industries must take responsibility for the security of their solutions, protect critical assets at the application layer on network attacks, promptly detect security threats, and quickly restore basic services.

Due to the complexity and massive number of 5G applications and contexts, application security requirements should at least apply a risk-based approach. This means that each security requirement is determined by an identified risk for risk mitigation. In general, the risk could be assessed by both the impact of an identified threat and the likelihood of this threat. Standards can be referred to do risk assessment such as:

- The ISO/IEC 27005:2018, Information Security Risk Management [7]. A risk assessment matrix in this standard can be referred.

Table 2 A Risk Assessment Matrix

Risk Assessment	Likelihood of incident scenario	Very Low (Very unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very low	0	1	2	3	4
	low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

In this perspective, OIC-CERT members should assess their 5G vertical markets' cybersecurity risk to determine the essential mitigation requirements.

There have been some cybersecurity related standards that are valid for vertical markets. For example, the ISO 62304 (secure development of medical device software), ISO 14971 (risk management of medical devices), ISA/ IEC 62443 EDSA (embedded device security assurance) are released to focus on healthcare cybersecurity. The ISO/ SAE 21434 is set for vehicle cybersecurity, while Open Web Application Security Project (**OWASP**) Internet of Things (**IoT**) verification standard ETSI EN 303 645 are for IoT cybersecurity requirements. These are all good baseline requirements that can be use as reference and the OIC-CERT members can develop additional requirement as per their individual assessment result.

Application security requirements is an open topic for policy makers, customers, and suppliers in the industry. Some key requirements are still valuable to consider, such as well-recognised standard adoption, and public and transparent certification.

For the application security requirements, there is one critical aspect that should be sufficiently considered, which is to what extent the application or a vertical industry of 5G is managed, operated, or enabled by the cloud computing and artificial intelligent (**AI**). With the 5G network, a large amount of data will be stored on the cloud and processed by AI. Some popular applications may be directly operated from the cloud and complex services are provided via the AI. Thus, cloudification might become a new trend for application layer. The application data has been facing serious threats on data breaching and abuse lead by cloud and AI.

Therefore, cybersecurity of either the cloud or AI would be increasingly critical to the security of the application layer in this framework. Related cloud and AI cybersecurity requirements and standards should be made a serious practice by the stakeholders.

4.4 A shared responsibility and collaboration

The 5G cybersecurity is under the shared responsibility of key stakeholders, including the MNOs, interconnection providers, vendors, application developers, service providers, and governments. Each of them should have clearly defined responsibilities, which, when fully met, can enable the deployment and operation of the 5G systems in a secure manner.

In the OIC-CERT 5G Cybersecurity Risk Repository, it is clear that counter measures against a same threat may involve more than one actors, which are government and national regulators, MNOs, equipment vendors, and service providers. For example, to prevent the DDoS attacks on core networks, government and national regulators could regulate the illegal act of initiating DDoS attacks against core networks and enforce penalties. Simultaneously, MNOs could deploy anti-DDoS devices at the network border and deploy security edge protection proxies and signalling firewalls. The vendor can develop flow control mechanism from core network elements. For the service providers, it is applicable to monitor application servers to prevent starting DDoS attacks.

The government and industry share similar goals in mitigating cybersecurity threats to the network infrastructures, preventing cyberattacks, and reducing the impact of illegal cyber behaviours. For the OIC-CERT 5G Cybersecurity Framework, achieving these goals would be a collective effort. The public-private partnerships should be leveraged to ensure that both the

government and industry arrive at the desired policy outcome of a more secure 5G networks. It is imperative that multiple sides work together to fully understand and assess potential threats to take the appropriate mitigation measures [8].

5 Certification

5.1 Need for Certification

After understanding the security requirements involved in the OIC-CERT Cybersecurity framework, it is still essential to assess if the targeted 5G cybersecurity requirements and standards are well deployed and implemented. Generally, a certification can reflect the level of accomplishment and perseverance. Certification can also be a differentiator for equipment vendors, network operators, and application service providers, by providing the extra marketability and professional cybersecurity capability, expertise, and conformance. From the perspective of the government and regulators, certifications can be a key factor to enhance the confidence for the 5G network operators, vendors, and application providers.

It is necessary to set the certification schemes for each security layer's security requirements and standards, accordingly. There are various security requirements and existing references of the three layers in the framework. This means that the OIC-CERT members need to decide on the exact certification schemes that are useful and essential for them. Therefore, it is unrealistic to design specific certification schemes in this document. It is only reasonable to design a unified certification mechanism as a guide for any possible certification schemes' deployment and implementation by the OIC-CERT members.

5.2 Certification Mechanism

5.2.1 Roles and responsibilities in certification scheme

- **Certification Body** (**CB**): Third-party conformity assessment body operating certification schemes. The CB oversees the activities of certification related to the issuance of certificates
- **Evaluation Body** (**EB**): Third-party conformity assessment body that performs one or more activities such as audit, test, and sampling associated with subsequent evaluating activities
- **Conformity Assessment Body** (**CAB**): A CAB accredits and supervises both the certification body and evaluation body
- **Provider/ Operator/ Vendor**: those who provides the 5G applications, or operates 5G networks, or provides network equipment.

5.2.2 Certification Mechanism Overview

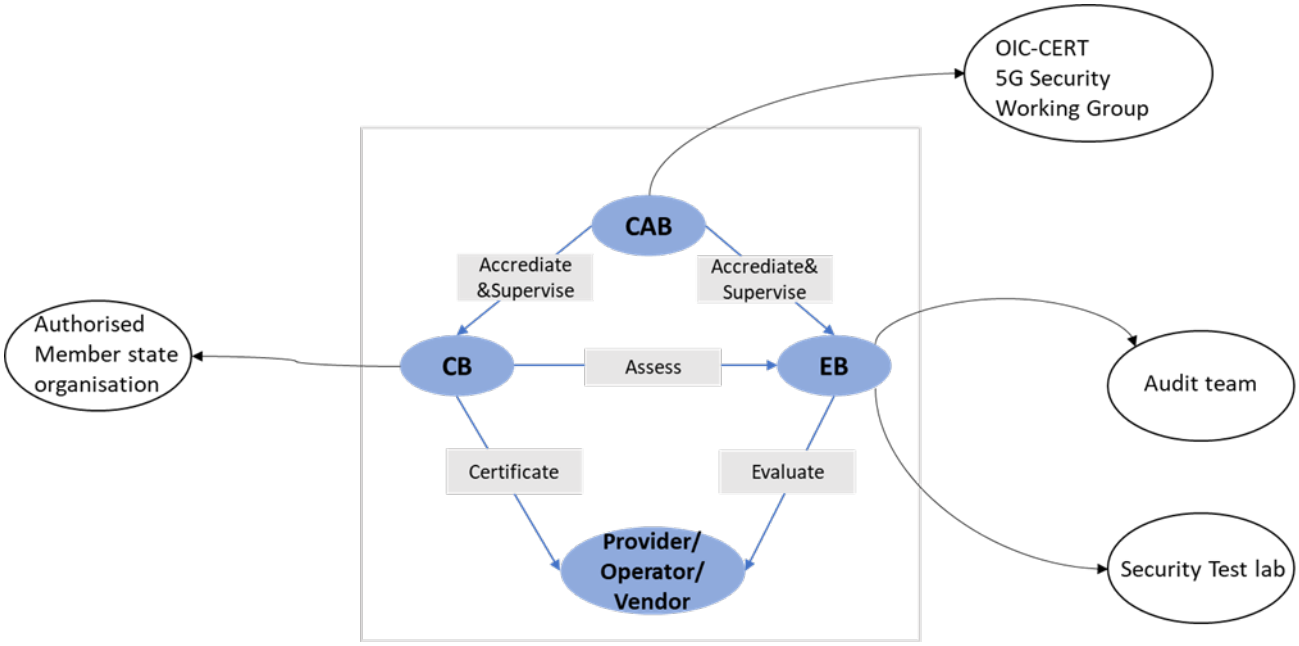

Figure 3 Certification Mechanism

Structurally, the CAB accredits and supervise the CB and EB, in the initial phase of developing the certification system. Then, the EB evaluates the equipment, network, and application's cybersecurity against the targeted requirements. At the same time, the CB should assess evaluation result's effectiveness provided by the EB, so that the CB can decide whether to certify the security level of the applicant's equipment, network or application.

According to this certification mechanism, organisations appointed as the CAB, EB, and CB can be:

- the OIC-CERT 5G Working Group as the CAB
- the Authorised OIC-CERT Members' organisation as the CB
- the audit team and security test lab as the EB

A network security certification example of such certification mechanism is shown below.

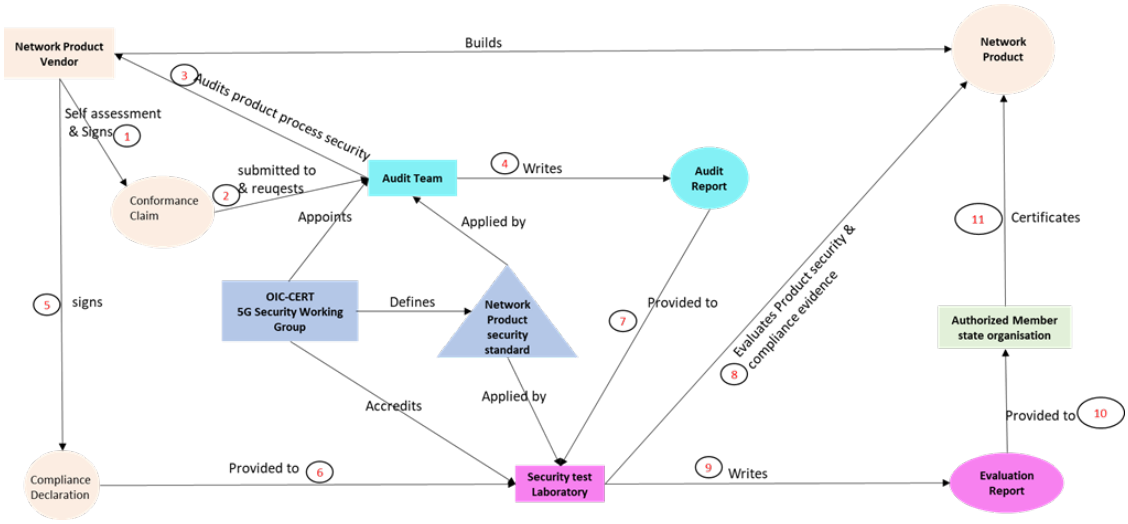

Figure 4 Example of a Network Equipment Security Certification

In this example, the CAB is the OIC-CERT 5G Security Working Group, the EB contains both audit team and security test lab. The CB is an authorized OIC-CERT members' organisation. The certification flow is summarized in the following table.

Table 3 Certification Flow

Steps	Description
1	The network equipment vendor starts the self-assessment and signs the conformance claim to prove that the equipment development and lifecycle conform to the security requirements defined in the standard
2	The conformance claim is submitted to an appointed audit team and the vendor apply for an equipment process audit
3	The audit team starts the audit on the applied equipment chosen by the vendor, which should be evidence based on site
4	The audit team writes the audit report. When all the requirements are satisfied can the chosen equipment's development and lifecycle process be compliant
5	The vendor begins to apply for the equipment's security assurance test to the lab
6	A compliance declaration including the evidence of the audited process should be submitted to the security test lab
7	The audit report should also be provided to the security test lab to support the compliance declaration
8	The test lab evaluate the audited processes base on the security requirements, and evaluate the security of the equipment
9	The security test lab provides an evaluation report to reflect how much the vendor has comply to the equipment security and equipment development and lifecycle process requirements.
10	The evaluation report is provided to the CB for certification purposes
11	The CB assesses the effectiveness of the evaluation report and decide whether to certify the chosen network equipment

For this example, there have been some existing standards or requirements that are able to be directly applied into certifying a network equipment. This document selects a few for reference purpose.

- GSMA FS.14 Network Equipment Security Assurance Scheme – Security Test Laboratory Accreditation and Product Evaluation [9]
- GSMA FS.15 Network Equipment Security Assurance Scheme – Development and Lifecycle Assessment Methodology [10]
- 3GPP TR 33.916 Assurance Methodology for 3GPP network products [11]