ITUPublications

International Telecommunication Union
Development Sector

Output Report on ITU-D Question 4/2

Telecommunication/ICT equipment: Conformance and interoperability, combating counterfeiting and theft of mobile devices

Study period 2022-2025

Output Report on ITU-D Question 4/2

Telecommunication/ICT equipment: Conformance and interoperability, combating counterfeiting and theft of mobile devices

Study period 2022-2025

Telecommunication/ICT equipment: Conformance and interoperability, combating counterfeiting and theft of mobile devices: Output Report on ITU-D Question 4/2 for the study period 2022-2025

ISBN 978-92-61-41181-7 (Electronic version)
ISBN 978-92-61-41191-6 (EPUB version)

Acknowledgements

The study groups of the International Telecommunication Union Telecommunication Development Sector (ITU-D) provide a neutral platform where experts from governments, industry, telecommunication organizations and academia from around the world gather to produce practical tools and resources to address development issues. To that end, the two ITU-D study groups are responsible for developing reports, guidelines and recommendations based on input received from the membership. Questions for study are decided every four years by the World Telecommunication Development Conference (WTDC). The ITU membership, assembled at WTDC-22 in Kigali in June 2022, agreed that, for the period 2022-2025, Study Group 2 would deal with seven Questions within the overall scope of digital transformation.

This report was prepared in response to Question 4/2: **Telecommunication/ICT equipment: Conformance and interoperability, combating counterfeiting and theft of mobile devices**, under the overall guidance and coordination of the management team of ITU-D Study Group 2 led by Mr Fadel Digham (Arab Republic of Egypt), as Chair, supported by the following Vice-Chairs: Mr Abdelaziz Alzarooni (United Arab Emirates), Ms Zainab Ardo (Federal Republic of Nigeria), Mr Javokhir Aripov (Republic of Uzbekistan), Ms Carmen-Mădălina Clapon (Romania), Mr Mushfig Guluyev (Republic of Azerbaijan), Mr Hideo Imanaka (Japan), Ms Mina Seonmin Jun (Republic of Korea), Mr Mohamed Lamine Minthe (Republic of Guinea), Mr Víctor Antonio Martínez Sánchez (Republic of Paraguay), Ms Alina Modan (Romania),[1] Mr Diyor Rajabov (Republic of Uzbekistan),[1] Mr Tongning Wu (People's Republic of China) and Mr Dominique Würges (France).

The report was developed under the leadership of the Rapporteur for Question 4/2, Mr Ibrahima Sylla (Republic of Guinea), the author of Chapter 1, with the participation of the following chapter authors: Vice-Rapporteurs Ms Tharalika Livera (Democratic Socialist Republic of Sri Lanka), author of Chapter 2; Mr Serigne Abdou Lahatt Sylla (Republic of Senegal), author of Chapter 3; Mr Junzhi Yan (People's Republic of China), author of Chapter 4; Ms Awa Koko Valéry Nadège Traore Epouse Goue (Republic of Côte d'Ivoire), author of Chapter 5; and Mr Sergei Melnik (International Telecommunication Academy), author of Chapter 6. The contribution of the following active contributors is also acknowledged: Mr Gordon Gillerman (United States of America) and Mr Turhan Muluk (Intel Corporation).

This report has been prepared with the support of the ITU-D Question 4/2 focal points, editors, the publication production team and the ITU-D Study Group 2 secretariat.

[1] Stepped down during the study period.

Table of contents

List of table and figures

Table

Figures

Executive summary

The general principles for the development of this report were 1) using conformance & interoperability (C&I) to improve access to information and communication technologies (ICTs) for citizens in developing countries, and 2) avoiding the creation of unnecessary barriers to trade.

This executive summary highlights the main issues raised in the Declaration of the eighth World Telecommunication Development Conference, held in Kigali, Republic of Rwanda, from 6 to 16 June 2022, under the theme ***"Connecting the unconnected to achieve sustainable development".*** Here are the main points raised:

- **Importance of ICTs:** ICT devices are essential in today's digital world.
- **Interoperability of networks:** the need for interoperability among international telecommunication networks was the main reason for creating the International Telegraph Union in 1865, and this remains one of the main goals in the ITU strategic plan.
- **Harmonization of standards:** global harmonization of standards is crucial to ensure the interoperability of networks and devices.
- **C&I programmes:** all countries implement C&I programmes, but at different paces. It is beneficial to leverage and recognize existing international practices, for example those established in the United States, the European Union and elsewhere.
- **ITU-D assistance:** ITU-D assists Member States in addressing technical and economic challenges related to the C&I of ICT devices.
- **Role of regulatory authorities:** regulatory authorities play a crucial role in managing C&I frameworks to ensure security and control.
- **Future developments:** the emergence of new technologies, especially those related to the Internet of Things (IoT), poses additional C&I challenges.
- **New network technologies:** there is a need to support Member States, in particular developing countries, in increasing awareness and understanding about disaggregated, open, and interoperable network technologies, such as open radio access networks (Open RAN) and others, by organizing workshops and other capacity-building activities.
- **Digital skills**: effective plans to develop and enhance the digital capacities and skills that are required in the online world, without which the digital divides will continue to widen.
- **Good practices:** the report examines good practices for finding optimal C&I solutions.

In summary, the report highlights the importance of assisting developing countries in the field of ICT C&I, as well as the challenges and opportunities associated with this evolving field.

Abbreviations and acronyms

Abbrevia-tions	Meaning	
3G	third generation mobile technology	
3GPP	Third Generation Partnership Project	
4G	fourth generation mobile technology	
5G	fifth generation mobile technology	
6G	sixth generation mobile technology[2]	
AB	accreditation body	
AI	artificial intelligence	
ANSI	American National Standards Institute	
ANSSI	National Agency for Information Systems Security of Guinea	
APIs	application program interfaces	
C&I	compliance/conformance/conformity and interoperability	
CAB	conformity assessment body	
DMIS	dimensional measurement interface standard	
DMSC	Digital Metrology Standards Consortium	
EMC	electromagnetic compatibility	
ETSI	European Telecommunications Standards Institute	
GDP	gross domestic product	
GDPR	General Data Protection Regulation	
GSMA	Global System for Mobile Communications Association	
HPHC	high processing and high connectivity	
IAF	International Accreditation Forum	
ICTs	information and communication technologies	

[2] While care was taken in this document to properly use and refer to the official definition of IMT-generations (see Resolution ITU-R 56, "*Naming for International Mobile Telecommunications*"), parts of this document contain material provided by the membership which refers to the frequently used market names "xG". This material cannot necessarily be mapped to a specific IMT-generation, as the underlying criteria from the membership are not known, but in general, IMT-2000, IMT-Advanced, IMT-2020 and IMT-2030 are known as 3G/4G/5G/6G, respectively.

(continued)

Abbreviations	Meaning	
IEC	International Electrotechnical Commission	
IECERS	Integrated Electronic Communication Equipment Registration System	
IEEE	Institute of Electrical and Electronics Engineers	
IETF	Internet Engineering Task Force	
ILAC	International Laboratory Accreditation Cooperation	
IMEI	international mobile equipment identity	
IMT	International Mobile Telecommunications	
ISDN	integrated services digital network	
ISO	International Organization for Standardization	
IoT	Internet of Things	
ITU	International Telecommunication Union	
ITU-D	ITU Telecommunication Development Sector	
ITU-R	ITU Radiocommunication Sector	
ITU-T	ITU Telecommunication Standardization Sector	
JTC	Joint Technical Committee	
KEBS	Kenya Bureau of Standards	
LEO	low-Earth orbit	
LoRaWAN	long range wide area network	
LPHC	low processing and high connectivity	
LPLC	low processing and low connectivity	
LPWAN	low-power wide area network	
LTE	Long-Term Evolution	
M2M	machine-to-machine	
MRAs	mutual recognition arrangements/agreements	
NCA	National Communications Authority of Ghana	
PDCA	plan, do, check, act	
QIF	quality information framework	

(continued)

Abbrevia-tions	Meaning	
RAN	radio access network	
RF	radio frequency	
SDGs	Sustainable Development Goals	
SIPs	session initiation protocols	
SWG 5	Special Working Group 5	
TBT	technical barriers to trade	
TIA	Telecommunications Industry Association	
TRCSL	Telecommunications Regulatory Commission of Sri Lanka	
W3C	World Wide Web Consortium	
WSN	wireless sensor network	
WTDC	World Telecommunication Development Conference	
WTO	World Trade Organization	
WTSA	World Telecommunication Standardization Assembly	

Chapter 1 – ICT products to achieve the Sustainable Development Goals

1.1 Introduction

The Sustainable Development Goals (SDGs) are at the heart of global efforts to address the most pressing challenges of our time, from poverty alleviation to environmental sustainability. Information and communication technologies (ICTs) play a crucial role in achieving these goals, providing tools and innovative solutions to address challenges in an effective and sustainable manner.

ICT products can contribute to all the SDGs. For example, mobile applications can be used to improve access to education, sensor-based monitoring systems can help manage water resources, and e-commerce platforms can foster inclusive economic growth.

In addition, ICTs can encourage collaboration and awareness by enabling individuals and organizations to exchange information, coordinate their actions and mobilize resources globally. This promotes a holistic and integrated approach to achieving the SDGs, fostering cooperation among governments, the private sector, civil society and citizens.

By investing in the development and use of ICT products to achieve the SDGs, the power of technology can be harnessed to create a more just, sustainable and prosperous future for all.

Figure 1: The Sustainable Development Goals

Source: United Nations[3]

[3] https://www.un.org/en/teach/SDGs

1.2 Relevance of ICT products to society

ICT products play a key role in our modern society and offer a host of benefits and opportunities. Their relevance to society can be observed at several levels:

- **Improved connectivity:** ICT products, such as smartphones and computers, facilitate communication and connectivity between individuals, communities and nations. This promotes information exchange, collaboration and the strengthening of social ties.
- **Access to information:** ICTs provide quick and easy access to a vast amount of information on a variety of topics, facilitating learning, research and informed decision-making.
- **Improving public services:** governments are using ICT products to improve the efficiency and accessibility of public services, such as e-health services, remote education systems, and transport management platforms.
- **Innovation and economic development**: ICTs drive innovation and economic development by facilitating the creation of businesses, making global markets easier to access, and automating business processes.
- **Social inclusion:** ICT products can help bridge the digital divide by providing equitable access to technology and connecting marginalized groups to economic and social opportunities.
- **Supporting the SDGs**: ICT products can be used to address many social and environmental challenges, such as alleviating poverty, promoting education, managing natural resources, and reducing inequalities.

As such, ICT products are important for society because they enable connectivity, access to information, efficient government services, economic innovation, social inclusion and the achievement of the SDGs.

1.3 Socio-economic applications of ICT devices

When a society's social targets are well-integrated and considered alongside economic viability, ICT devices can help combine the principles of social enterprise with the possibilities offered by technology to create a positive and sustainable impact on society. Here are some ways by which ICT devices can be used in this context:

- **Expanded accessibility**: by using ICTs, socio-economic initiatives can expand their impact by reaching a wider audience. Technologies such as affordable smartphones and computers can make services accessible to more people, including those from marginalized or low-income communities.
- **Social innovation:** ICT devices are enabling the development and implementation of innovative solutions to respond to social problems. For example, mobile applications can be designed to provide affordable health care services in rural areas or facilitate access to education in disadvantaged communities.
- **Capacity building:** ICT equipment and devices can be used to strengthen the capacities of socio-economic organizations by equipping them with management, monitoring and evaluation tools. Project management software, data collection platforms and online communication tools can help these organizations optimize their operations and measure their impact.
- **Digital inclusion:** by providing training on the use of ICT devices and digital skills, socio-economic initiatives can promote digital inclusion and bridge the digital divide in communities.

- **Bridging the gender divide:** ICTs and ICT products are an essential pathway to gender equality and the empowerment of all women and girls.
- **Environmental sustainability:** ICT devices can also be used in an environmentally responsible manner in a socio-economic society. For example, recycling initiatives for electronics can help reduce e-waste and promote environmental sustainability. By integrating ICT devices into a socio-economic society model, innovative, accessible and sustainable solutions can be created to meet the social, economic and environmental needs of communities.

The benefits associated with the use of ICT products are increasingly well-received by developing countries, most of which are embarking on vast ICT development programmes.

It is against this backdrop that the Central African Republic[4] is tackling major regulatory and institutional gaps in order to take full advantage of digital technologies as an engine of growth and a tool to support poverty reduction. The ultimate objectives are to resolve the problems associated with counterfeit and falsified ICT equipment and, above all, to achieve the SDGs relating to industry, innovation and infrastructure (SDG 9) by 2030.

Ultimately, in the hope of supporting technological research, development and innovation at the national level and significantly increasing public access to affordable broadband technologies and services, the Central African Republic has decided to:

a. improve the legal and regulatory framework of the telecommunication sector;
b. strengthen the capacities of its Ministry of the Digital Economy, Posts and Telecommunications and its telecommunication regulatory authority, the Regulatory Authority for Electronic Communications and Posts;
c. establish an adequate accredited laboratory to test or recognize ICTs equipment;
d. promote the sharing and deployment of telecommunication infrastructure by the Regulatory Authority in order to reduce deployment costs.

1.4 Adherence to recognized standards / compliance with recognized ICT standards for quality and interoperability

In the context of ICTs for society, adherence to recognized standards is of paramount importance to ensure the quality, security and interoperability of products and services. Examples of recognized standards that ICT products must comply with include:

- ISO 27001 – information security: This International Organization for Standardization (ISO) standard defines the requirements for the implementation, maintenance and improvement of an information security management system. It aims to protect sensitive information from threats such as hacking, data loss, and privacy breaches.
- ISO 9001 – quality management: The ISO 9001 standard establishes the criteria for an effective Quality Management System (QMS). It is aimed at suppliers of ICT products to ensure customer satisfaction, continuous improvement and regulatory compliance.
- The World Wide Web Consortium (W3C) establishes standards and recommendations for the development of web technologies, such as HTML, CSS, and JavaScript. Adherence to these standards ensures that ICT products are compatible with modern web browsers and accessible to a wide audience.

[4] Document SG2RGQ/17 from the Central African Republic.

- General Data Protection Regulation (GDPR): it is essential for ICT products that process personal data to comply with the GDPR to ensure respect for the users' rights to privacy and data protection.
- The Institute of Electrical and Electronics Engineers (IEEE) sets standards for various aspects of ICT, including wireless networking, Ethernet communications, and coding standards.
- ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories: this ISO and International Electrotechnical Commission (IEC) standard specifies the general requirements for the competent, impartial and consistent operation of laboratories. Laboratory customers, regulatory authorities, organizations and schemes using peer-assessment, accreditation bodies (ABs), and others use this document for confirming or recognizing the competence of laboratories. By having their ICT products tested in competent laboratories (as per standards like ITU Telecommunication Standardization Sector (ITU-T) Recommendations) that are accredited by ABs that are signatories to the International Laboratory Accreditation Cooperation Mutual Recognition Arrangement (ILAC MRA), ICT suppliers gain the trust of customers with regard to C&I.
- 5G (International Mobile Telecommunications (IMT)-2020) and 4G Long-Term Evolution (LTE) standards for high-speed mobile communication.
- ISO/IEC 17788 & ISO/IEC 17789 for cloud computing and reference architecture standards.
- ISO/IEC 22989 standard for artificial intelligence (AI) terminology and concepts.

Table 1: Organizations producing or recognizing international standards

No	Organization	Description	link
1	ITU	The International Telecommunication Union develops global standards for telecommunications and ICTs.	https://www.itu.int/ITU-T
2	ISO	The International Organization for Standardization publishes international standards for various industries, including ICTs.	https://www.iso.org
3	IEC	The International Electrotechnical Commission focuses on standards for electrical, electronic and related technologies.	https://www.iec.ch
4	IEEE	The Institute of Electrical and Electronics Engineers develops standards for a wide range of industries, including ICT and networking.	https://www.ieee.org
5	ETSI	The European Telecommunications Standards Institute produces standards for ICT systems and services in Europe and around the world.	https://www.etsi.org
6	ANSI	The American National Standards Institute oversees the development of voluntary consensus standards in the United States.	https://www.ansi.org
7	W3C	The World Wide Web Consortium develops standards for the web, ensuring its long-term growth and interoperability.	https://www.w3.org

Key points:

- **Adherence to standards** ensures that ICT products and services meet global benchmarks for quality, security and interoperability.
- **Compliance** demonstrates alignment with internationally recognized standards, facilitating market access and user trust.
- **Interoperability** enables seamless integration and communication between different systems and technologies.

More partnerships and information exchanges need to be developed with key external organizations that play a critical role in standards development and international accreditation. Here are some courses of action:

- **Establish dedicated contact points** with organizations such as IEEE, ISO, IEC and the Internet Engineering Task Force (IETF), to facilitate regular information-sharing.
- **Actively participate in forums and working groups** (the Third Generation Partnership Project (3GPP), the Internet Task Force, IEEE etc.) to ensure that local needs are better integrated into international standards.
- **Create follow-up mechanisms** to collect relevant data from these external budgets and incorporate them into future reports.
- **Strengthen liaisons between institutions** through cooperation agreements or strategic partnerships to ensure the mutual exchange of expertise and resources.

Global assessment programmes need to be adaptable and forward-looking, such as those of Wi-Fi Alliance. Here are some possible actions:

- **Identify specific programmes:** for example, the Wi-Fi CERTIFIED® certifications issued by Wi-Fi Alliance ensure product interoperability, security and performance.[5]
- **Highlight their importance:** describe how these programmes promote the adoption of standards and ensure compatibility between different equipment and technologies.
- **Integrate other similar initiatives**: mention programmes such as the Bluetooth Special Interest Group (SIG), LoRa Alliance, or other consortia working on the interoperability of emerging technologies.
- **Analyse regional impact:** assess how these programmes influence local markets and their relevance to the technological and economic development of the region in the report.

To harness the transformative potential of digital platforms and processes, several development avenues should be considered:

- Define digital platforms: explain what a digital platform is, how it facilitates the interconnection of different actors, products and services (e.g. payment platforms, communication platforms and e-commerce).
- Present the benefits of digital platforms:
    1. **Improved efficiency:** optimizing business processes and reducing of operational costs.
    2. **Increased accessibility:** facilitating access to remote services, thereby increasing inclusivity and connectivity.
    3. **Continuous innovation**: Enabling the rapid development of new products and services through the integration of emerging technologies.

[5] https://www.wi-fi.org/certification

- Explore digital processes:
  1. **Process automation:** integrating automation technologies to improve productivity and reduce human error.
  2. **Transformation of business models:** adopting digital tools to facilitate information management, communication and collaboration within business and public administrations.
  3. **Digitalization of public services**: discussing the impact of the digital transformation of government services (e.g. e-government, e-health, e-education).
- Examples of successful digital platforms and processes:
  1. **Collaborative platforms**: such as those used for e-education or telemedicine.
  2. **Digital processes in the public sector:** the implementation of digital public services to facilitate administrative procedures.
  3. **Specific sectors:** applications in the finance (Fintech), transport (Mobility as a Service) sectors, etc.
- Challenges and opportunities:
  1. **Challenges**: data security, cybersecurity, privacy, infrastructure requirements and digital inclusion.
  2. **Opportunities:** creating digital economies, improving competitiveness and boosting innovation.

1.5 Impact of the COVID-19 pandemic on approval procedures

The COVID-19 pandemic has had a significant impact on authorization procedures in many areas, including in the field of ICTs. Some of the main consequences of the pandemic on these procedures include:

- **Adoption of digital procedures:** with travel restrictions and social distancing measures, many authorization procedures have been fully digitized. Authorities have set up online platforms to submit and process permit applications, reducing the need for physical documents and face-to-face meetings.
- **Faster processing times:** in many cases, the pandemic has accelerated licensing processing times, as governments have sought to facilitate the rapid deployment of ICT solutions to address urgent pandemic-related needs, such as teleworking, e-learning and telemedicine.
- **More flexibility:** the authorities have shown greater flexibility in assessing authorization applications given the exceptional circumstances related to the pandemic. In some cases, this has led to procedures being simplified or eligibility criteria relaxed in order to encourage innovation and the rapid implementation of technological solutions.
- **Increased security:** despite the shift to digital processes, authorities have also strengthened security measures to protect sensitive data and prevent misuse. This involved implementing robust security protocols to ensure the integrity and confidentiality of the information submitted as part of the authorization requests.
- **International collaboration:** the pandemic has encouraged greater international collaboration in the assessment and regulation of ICTs. Authorities shared good practices, data and resources to address the common challenges posed by the pandemic and promote a coordinated approach on a global scale.

Chapter 2 – Conformance and interoperability

2.1 Introduction

The telecommunication/ICT sector is evolving rapidly, driven by innovations in products, services and infrastructure. As these technologies become interconnected, it is essential for stakeholders to ensure C&I. Conformity assessment provides assurance that ICT equipment conforms to technical specifications and standards, which is essential for performance assessment and compatibility in network environments. Interoperability testing ensures that multiple products can integrate and communicate seamlessly, supporting specific communication protocols. Interoperability testing is designed to determine whether two or more products meet the technical specifications needed for successful integration by following specific communication protocols in the telecommunication and ICT sectors, drawing on the knowledge of international organizations such as ITU and regional working parties. It highlights the complex landscape in which C&I initiatives operate, from legacy network signalling issues to the proliferation of counterfeit mobile phones. This chapter also covers mutual recognition arrangements/agreements (MRAs) for conformity assessment, facilitating the cross-border recognition of test results and certification and encouraging international trade and cooperation. It also highlights the role of pre-conformity testing in proactively assessing product compliance with applicable standards, and the importance of market surveillance and raising awareness among suppliers and users to meet quality standards and combat counterfeit products.

MRAs can be multilateral between ABs who are peer-evaluated for their equivalence in assessing the competence of conformity assessment bodies (CABs), such as laboratories which test ICT products. Such MRAs help with the mutual acceptance of test results in economies that members represent, which can help in overcoming technical barriers to trade (TBTs). MRAs can also be concluded between governments in order to promote trade through the mutual acceptance of products with test reports from their respective economies' laboratories accredited by their national AB.

Mandatory verification of ICT equipment compliance is a crucial tool for ensuring the integrity, stability and security of telecommunication networks. However, it is essential to reduce the number of checks and shorten the time-to-market for ICT equipment. MRAs for test results from foreign laboratories can help, but the process is often costly and time-consuming due to the need for apostilled translations of test protocols.

A potential solution is the establishment of national ICT expertise, where a government-approved entity assumes responsibility for compliance verification. This approach minimizes examination time and costs, as it does not require full equipment testing. The cost of such examinations is significantly lower than conducting comprehensive ICT equipment tests.

1. C&I:

- Compliance testing ensures ICT equipment meets technical standards and specifications.
- Interoperability tests verify that products can integrate successfully within a network.

- These tests are vital for identifying non-compliant equipment that could compromise network quality.

2. Technical specifications and standards:

- Standards are set by service providers, operators and national regulators.
- Compliance with these standards ensures interoperability, reduces vendor lock-in and promotes market competitiveness.
- The Technical Barriers to Trade Committee of the World Trade Organization (WTO) emphasizes transparency, openness, impartiality and consistency in standard development.

3. MRAs:

- MRAs facilitate the recognition of compliance test results between countries, reducing redundant testing and costs.
- The aim is for one test to be accepted everywhere; however, MRAs face challenges such as legal barriers, lack of reciprocity, and insufficient resources in some countries.

4. National ICT expertise:

- A national ICT expertise system can ensure compliance with both national and international standards.
- It establishes accountability, prevents the counterfeiting of products and reduces costs by avoiding full-scale testing.
- This system requires a regulatory framework, accreditation rules and qualified experts.

5. Challenges and solutions:

- Differences in ICT implementation across countries complicate mutual recognition.
- National expertise systems can address these challenges by providing localized compliance verification.[6]

2.2 Consideration of key issues

Interoperability problems in the signalling of existing intelligent networks can be attributed to different factors:

1. lack of C&I between equipment from different vendors;
2. non-standard interfaces or protocols; and
3. software revisions from a single manufacturer.

This may result in incompatible session initiation protocols (SIPs). Voice, data and video capacity may also be affected by the overload of the existing network. Interoperability in complex networks can be achieved through the integration of networks and devices. However, some vendors may not provide the necessary infrastructure and support teams for interoperability with other operators. The adoption of standards, the management of call detail records and the implementation of new features and services across all platforms also pose challenges. In addition, there is a lack of test centres and trained personnel, and there are also problems with integrated services digital network (ISDN) support, user terminals, and the interoperability of services and terminal equipment used by customers.

[6] ITU-D SG2 Document 2/140 from the International Telecommunication Academy.

In addition, some challenges were identified at the regional and national levels, including:

- lack of regional collaboration in the development and implementation of counterfeit phone solutions;
- absence of baseline data to inform the development and implementation of strategies to combat regional trade in counterfeit devices;
- persistent challenges related to the affordability of mobile phones;
- low level of awareness of counterfeit phones;
- counterfeit devices that are a potential threat to the national digital transformation plans of developing countries;
- the economic impact of counterfeit devices, which can also reduce the contribution of a country's ICTs sector to gross domestic product (GDP); and
- counterfeit devices that compromise security, network performance and quality of service and predispose populations to a multitude of health risks.

The increased demand for mobile phones and their permanent ownership transcends both geographical factors, such as urban and rural communities, and societal factors, such as income variability and literacy level, but together they may be drivers for the influx of counterfeit mobile phones into the market.[7]

2.3 Technical specifications and standards

2.3.1 Demonstration of C&I applications at national and regional levels

Demonstrating the applications of C&I is crucial for understanding national and regional experiences and promoting good practices. These include designation/recognition of accreditation and certification bodies, of international standards and practices, and of testing laboratories, along with registration and certification. Such demonstrations can provide valuable insights into successful implementation strategies, challenges faced and lessons learned.

One of the prerequisites for the designation or recognition of an AB is whether it is a signatory to the ILAC/International Accreditation Forum (IAF) MRA, which provides formal attestation that its processes and criteria meet international standards for certification bodies and testing laboratories.

Sharing the stories of ABs that have been successful in promoting conformity assessment practices and facilitating market access for compliant products and services can build trust and reduce barriers to trade. The designation/recognition of certification bodies is carried out in order to establish the procedures and requirements for assessing the conformity of a product with the applicable standards and regulations.

Demonstration of competence, impartial and consistent operations of testing laboratories can build trust with regard to their capability to generate valid test results. In cases where it is difficult to establish a national programme that includes all the various elements, countries can rely on the good practices and even certification from established programmes.

Registration/certification explains the processes and criteria for registration or certification of products, services or systems that demonstrate compliance with applicable regulations and

[7] ITU-D SG2 Document SG2RGQ/37 from Zambia.

standards. Showcasing certified products can show how registration or certification marks are symbols of quality, safety and reliability, enabling consumers to make informed purchases. Recognition of certification marks from established, well-managed and internationally recognized programmes as demonstration of conformance can greatly reduce cost, time to consumer, as well as cost to the national administration.

2.3.2 Good practices

- **Issuance of reseller certificates**: ensure that resellers of ICT devices obtain officially recognized certificates to enhance transparency and compliance.
- **Creation of an integrated registration system**: establish a comprehensive reference and registration system for electronic communication equipment to improve traceability and regulatory oversight.
- **Consumer access to international mobile equipment identity (IMEI) verification**: provide consumers with an easily accessible means to verify IMEI numbers through a short code, enhancing device authentication and helping prevent fraud.
- **Regional reporting on counterfeit trends**: facilitate the availability of regional reports on reported volumes and trends (e.g. phone models most susceptible to counterfeiting) to raise consumer awareness.
- **Recognition of international testing and certification standards**: ensure that test results and certifications adhere to international standards and good practices for greater interoperability and market acceptance.

2.3.3 Possible collaborative mechanisms for the establishment of joint C&I

Service providers and operators implement harmonized standards and specifications for the equipment and systems they use to serve their customers. National regulators establish regulations for harmonized standards and specifications of equipment and systems deployed within their national borders. Users, service providers and national regulators must obtain irrevocable proof that such equipment and systems conform to the appropriate interoperability standards, requirements and specifications.

In order to promote the development of international standards, guides and recommendations, the TBT Committee of the World Trade Organization has established the following six principles:

1. **Transparency:** This principle requires that all essential information concerning ongoing work programmes, as well as proposals for standards, guides and recommendations under consideration and the final results, should be made readily available to at least all interested parties in the territories of at least all WTO members. It encourages the establishment of procedures that provide sufficient time and opportunity for the submission of written comments. Information on these procedures should be disseminated effectively.

   To provide essential information, transparency procedures should: provide sufficient time for interested parties to submit written comments and take them into account in the subsequent consideration of the standard; promptly publish standards upon adoption; and periodically publish a work programme containing information on standards under development or in the process of adoption.
2. **Openness:** This principle requires that membership of an international standardizing body should be open, without discrimination, to the relevant bodies of at least all WTO members, both for participation at the policy development level and for each stage of standards development.

As such, any member of the international standardizing body, particularly developing countries, with an interest in a specific standardization activity, should be given meaningful opportunities to participate in all stages of standards development.

3. **Impartiality and consensus:** This principle emphasizes the opportunity for all relevant bodies of WTO members to contribute meaningfully to the development of an international standard, so that the process of developing the standard does not privilege or favour the interests of one or more particular suppliers, countries or regions. It recognizes that consensus procedures should be established to take into account the views of all parties concerned and to reconcile conflicting arguments.
4. **Effectiveness and relevance:** International standards should be relevant and respond effectively to regulatory and market needs, as well as to scientific and technological developments in individual countries, in order to facilitate international trade and prevent unnecessary barriers to trade.

   They should not distort the global market, adversely affect fair competition or stifle innovation and technological development. Furthermore, they should not favour the characteristics or requirements of specific countries or regions when different needs or interests exist in other countries or regions. As far as possible, international standards should be based on performance rather than design or descriptive characteristics.
5. **Consistency:** This principle requires international standards bodies to avoid overlap or duplication with the work of other international standards bodies in order to avoid the development of conflicting international standards. In this respect, cooperation and coordination with other relevant international bodies is essential.
6. **Development dimension:** this principle suggests that the constraints faced by developing countries, in particular those which prevent them from participating effectively in the development of standards, should be taken into account in the standards development process. As such, it encourages the search for ways to facilitate the participation of developing countries in the development of international standards, such as the use of technical assistance and capacity building.

2.3.4 Technical cooperation

- **Capacity building and training**: develop national and regional projects, along with training activities, to support governments in implementing effective measures against the influx of counterfeit devices.
- **Policy and regulatory support**: assist in formulating and strengthening policies, regulations, and enforcement mechanisms to curb the circulation of non-compliant ICT devices.
- **Cross-border collaboration**: foster cooperation between regulatory bodies, law enforcement agencies and industry stakeholders at national and regional levels to enhance anti-counterfeiting efforts.
- **Technology and infrastructure enhancement**: support the deployment of advanced technologies for device authentication, tracking and verification to improve market integrity.

2.4 Mutual recognition arrangements/agreements on conformity assessment

2.4.1 What is a mutual recognition arrangement/agreement?

MRAs are contractual agreements (on procedures and processes) between parties (private or public entities) regarding the recognition of conformity assessment results.

- **Mutual trust** strengthens technical cooperation between regulatory authorities.

Recommendation ITU-T Q.4068 presents a set of open APIs for interoperable testbed federation that are able to handle not only the interconnection and interoperability of testbeds within a federation, but also manage the announcement, allocation, and provisioning of resources. APIs are designed to manage the users involved in the federation, such as experimenters, and to assign roles to users. Similarly, the resource usage is assigned to an experimenter through the open APIs for interoperable testbed federation. A typical use case of an experiment is a testbed federation and related requirements. Similar use cases can be implemented in a testbed federation like Fed4FIRE.

2.4.2 Role of MRAs in C&I

MRAs are used to:

- recognize the competence of third parties to carry out national regulatory or licensing processes;
- avoid the costs of redundant tests and promote transparency;
- facilitate access to foreign markets;
- Reduce time-to-market and production costs;
- combat predatory practices and remove barriers to market entry;
- streamline procedures and methods, significantly reducing costs for producers in several markets.

The ultimate goal is for products to be tested once, accepted everywhere.

2.4.3 Issues related to international MRAs

Unfortunately, the use of MRAs often encounters difficulties:

- Many countries do not have a legal mechanism to use documents drawn up in another country and do not have apostilled translations in the language used by the target country.
- Not all countries have the material and human resources needed to carry out their own tests. In this case, mutual recognition of the results of tests and studies cannot be achieved, and unilateral recognition would not be acceptable. In these cases, countries can recognize test results and certifications from national or international administrations with reputable, well-established and documented national or regional programmes. This will permit the lawful use of all test and research results based on expert opinion from an organization authorized by the country's communication administration.
- ICTs vary from country to country. The country's communication administration sets the ICT implementation targets. Compliance with ICT usage objectives should be carried out by an agency authorized by the country's communications administration.

– In the case of contention, which can result in damages due to error in the outcome of tests and studies, it is very difficult to prosecute an organization that is working in accordance with the laws of another country.

In view of the above, there is a need to develop and universally apply a mechanism for national expertise on test results and studies. At the same time, the organization providing an expert opinion is held responsible in accordance with the law of the country in which it operates. It is also important to benefit from the good practices and experiences of countries that are successfully implementing MRAs.

2.5 Need for a strong C&I framework

2.5.1 Basic infrastructure for a quality C&I framework: technical standards and necessary legislative revisions

A robust C&I framework is essential for ensuring the seamless integration of ICT systems, fostering innovation and protecting consumers. Developing countries often face challenges in establishing such a framework due to gaps in technical standards, regulatory requirements, and legislative policies. A well-structured infrastructure, incorporating technical, legislative and regulatory aspects, is crucial for the effective implementation of C&I programmes.

Objective

The primary objective of this section is to highlight the fundamental infrastructure necessary for a quality C&I framework. This includes the establishment of the technical standards, regulatory mechanisms and legislative revisions required to support conformity assessment and interoperability in developing countries. Strengthening these elements will enhance the reliability, safety and efficiency of ICT ecosystems.

Impact

A well-defined C&I infrastructure has significant socio-economic and technological impacts. It ensures the interoperability of ICT solutions, reduces market barriers, enhances consumer confidence and promotes fair competition. Additionally, it facilitates international trade by aligning national standards with global good practices, enabling developing countries to participate more effectively in the global digital economy.

Role

By addressing these key areas, developing countries can create a strong foundation for a quality C&I framework, ultimately driving digital transformation and economic growth.

2.5.2 Concept of federation testing

Recent technological developments concerning the Internet have become more complex to test and use in the real world. A wider variety of conditions needs to be taken into account, and scalability evaluated. The need for experimentation within test benches has become more important for testing new use cases in real-world conditions. This development makes it increasingly necessary and practical to require and interconnect different testbeds. However, this powerful method lacks clearly standardized APIs to support this federation of existing testbeds

and resources to support the experimentation, testing and validation of new technologies, services and solutions to improve testbed interoperability.

2.6 Market surveillance

2.6.1 Awareness for better monitoring

Awareness among vendors and users of terminal equipment is crucial to improve the oversight of standards in the telecommunication industry. This not only improves product quality and reliability, but also promotes interoperability, regulatory compliance and consumer confidence. Suppliers can foster a culture of quality and reliability by understanding relevant standards, resulting in higher product quality, fewer defects and increased reliability. Users can make informed purchasing decisions and choose the products that meet their needs and expectations, resulting in increased satisfaction and confidence in the reliability and performance of the terminal equipment.

Vendors can promote interoperability by designing products that comply with industry standards and protocols, facilitating seamless communication and compatibility between different systems and platforms. Users benefit from the knowledge of regulatory standards, as it helps to ensure that their terminal equipment complies with the safety, security and privacy requirements imposed by regulatory bodies.

Gaining the trust of consumers is essential for suppliers, as it demonstrates their commitment to quality, reliability and customer satisfaction. Savvy users are more likely to trust equipment that conforms to recognized standards and certifications, fostering loyalty and positive brand perception. Market surveillance is essential to the proper functioning of the telecommunication marketplace, as it protects consumers and workers from the risks posed by non-compliant products, and protects companies from unfair competition.

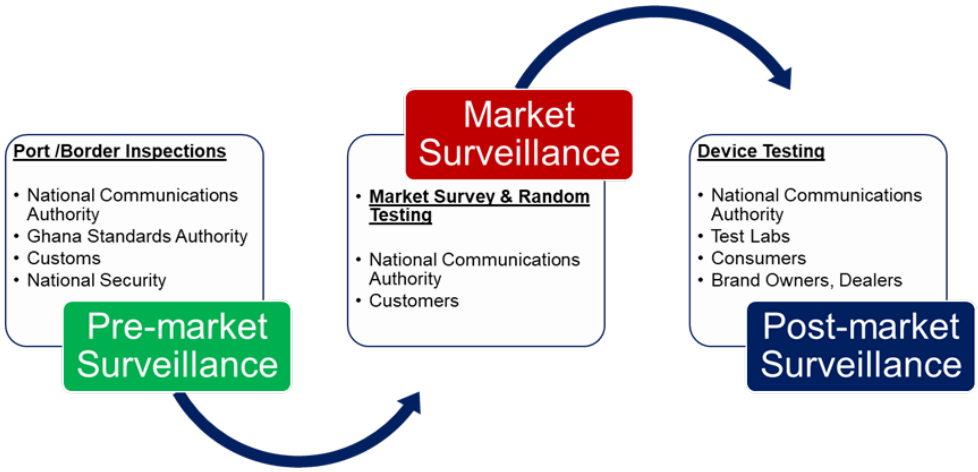
Market surveillance: this procedure is conducted to ensure that electronic communications equipment placed or used on the market conform to the pre-market approved standards.[8]

Three-pronged approach:

- Pre-market surveillance, including entry clearance procedures and physical port inspections;
- Market surveillance, including market surveys and random testing;
- Post-market surveillance activities.

[8] Roland Yaw Kudozia. Ghana. Combating counterfeit ICT devices through C&I testing and market surveillance. ITU-D Workshop on conformance and interoperability challenges for digital transformation, Geneva, 2 June 2023.

Figure 2: Promotion of market surveillance in Ghana



2.6.2 Monitoring and cooperation

Market surveillance intelligence and experience are essential to ensure regulatory compliance, fair competition and consumer interests in the telecommunication sector. By exchanging information, consulting with other countries and providing early warnings, regulators can strengthen market surveillance efforts, streamline enforcement activities and foster collaboration between parties. Knowledge exchange and regional cooperation are key assets of such consultations.

Regulators can benefit from sharing good practices, lessons learned and regulatory knowledge with other countries. This can lead to regional cooperation, the harmonization of regulatory approaches and the promotion of consistent enforcement and can help prevent regulatory fragmentation. Consultations also provide capacity-building opportunities, enabling regulators to better understand emerging technologies, trends and enforcement techniques.

Early warnings can be sent to partners to mitigate risk, optimize resource allocation and facilitate compliance. These warnings also serve as educational tools, raising awareness of regulatory requirements and encouraging voluntary compliance. By providing clear guidance and timely information, regulators enable parties to align their activities with regulatory expectations, mitigate compliance risks and help level the playing field in the marketplace.

Main stakeholders involved:

- governments/regulators;
- ABs;
- CABs;
- manufacturers, importers, vendors and service providers.

2.7 Conformity assessment of new technologies

Conformity assessment is an essential tool to ensure that new telecommunication/ICTs comply with industry standards, legal requirements and customer expectations. In the age of connected devices and networks, it is essential to ensure security, reliability and interoperability.

Policy-makers, businesses and consumers can be reassured about the performance and quality of telecommunication and ICT goods and services through conformity assessment.

Conformity assessment encompasses a number of approaches for assessing the various characteristics of ICTs and telecommunication technologies. These methods include accreditation, certification, testing and inspection. In order to determine if a product or system meets the established technical criteria, it undergoes testing, which involves subjecting it to rigorous examination in controlled environments. The main objectives of the inspection are to confirm compliance through visual inspection, documentation review and on-site assessments. The issuance of licences or official declarations attesting to compliance with specific rules or laws constitutes the certification process. Testing, inspection and certification activities are carried out by CABs, which are proven to be impartial and competent, and recognized as part of the accreditation process.

Internationally recognized standards and a sound regulatory framework are prerequisites for an effective conformity assessment. Regulatory bodies establish standards and guidelines to ensure the interoperability, security and safety of telecommunication and ICTs systems. To promote compatibility and facilitate global harmonization, standards bodies such as ITU, IEEE, IETF, IEC, the European Telecommunications Standards Institute (ETSI) and ISO develop technical specifications and protocols. Adherence to these guidelines encourages innovation while ensuring consistency and accountability throughout the ICT and telecommunication sector.

2.7.1 New technological challenges

Complexity of emerging technologies

The complexity of new ICTs and telecommunication technologies is one of the major obstacles to conformity assessment. The diversity in terms of the components, protocols and capabilities of technologies such as AI and IoT poses challenges for the development of standardized testing techniques. The rapid evolution and diversity of these technologies may make it difficult to maintain traditional conformity assessment techniques, which could lead to gaps in the assessment of the conformity of these technologies with defined standards. Modern telecommunication systems are interconnected, which adds additional levels of complexity. Therefore, there is a need for comprehensive assessment frameworks that take into account interoperability and system-level factors.

Lack of harmonized standards

The lack of uniform standards across jurisdictions and regions is a major obstacle. International borders are crossed by products and services offered on the global telecommunication/ICT markets. However, the variety of legal frameworks and standards creates difficulties for the mutual recognition and interoperability of conformity assessment results. Differences between standards can lead to market fragmentation, increased costs of conformance, and the duplication of testing efforts. To promote interoperability, facilitate international trade and reduce regulatory barriers in the telephony and ICT sectors, the harmonization of standards and MRAs are needed.

Rapid technological obsolescence

Rapid technical obsolescence is an obvious obstacle to conformity assessment in the ICT and telephony sector. Current standards and test procedures are often rendered obsolete by new technologies, requiring continuous updating and adjustment. To remain relevant and effective, CABs need to adapt quickly to new technologies and evolving regulatory requirements. But this constant need to adapt could put pressure on knowledge and resources, especially for small conformity assessment businesses. In addition, the short lifespan of some technologies could limit the accessibility of test equipment and reference materials, which would make conformity assessment initiatives even more challenging.

Interoperability and compatibility issues

In the conformity assessment of ICTs and telecommunication technologies, interoperability and compatibility issues are significant hurdles. Seamless interoperability is essential to providing reliable and consistent services across an interconnected ecosystem of diverse devices, networks and platforms. However, interoperability testing can be challenging and resource-intensive, especially in heterogeneous environments with proprietary protocols and outdated systems. Interoperability efforts are further hampered by the lack of standardized interfaces and protocols, resulting in gaps in interoperability and service disruptions. To overcome these obstacles, conformity assessment must implement detailed testing procedures that emphasize interoperability between the different levels of the ICT and telecommunication stack.

2.7.2 Pre-compliance testing

Pre-compliance testing is a proactive strategy used by manufacturers to assess the compliance of their products with applicable standards and regulations before pursuing official certification. With pre-conformance testing, manufacturers can detect potential compliance issues early in the development cycle, including time-to-market delays and frequently recommended redesigns or recalls. In addition, pre-compliance testing gives manufacturers insight into the performance characteristics of their products, ensuring optimal functionality and reliability. Pre-compliance testing helps manufacturers remain agile and adaptable in the rapidly changing telecoms and ICTs sectors, where standards are constantly evolving, and innovation is developing rapidly.

Pre-compliance testing involves identifying the standards and regulations governing a specific telecommunication/ICT device. Based on these standards, a comprehensive test plan is developed, describing specific tests and assessments. The test setup is crucial for accurate and reliable results. Pre-compliance testing includes electromagnetic compatibility (EMC) testing, electrical safety testing, radio frequency (RF) performance testing and environmental testing. Data is recorded and analysed against predefined acceptance criteria, allowing deviations from the standard to be identified and compliance status determined. Manufacturers can correct nonconformities by redesigning components, adjusting parameters or improving shielding. Comprehensive documentation is prepared throughout the process, detailing test procedures, results, corrective actions and observed deviations or anomalies. Iterative testing is often used to refine products, resolve remaining nonconformities and optimize performance. This process helps manufacturers to fine-tune their products and ensures compliance with applicable standards and regulations.

The pre-compliance testing of telecommunication and ICT devices must adhere to good practices and industry standards. These include early engagement with regulatory experts, full

test coverage, regular calibration and validation, realistic test scenarios, collaboration across cross-functional teams, and robust documentation management and tracking. Early engagement provides a better understanding of regulatory requirements and streamlines the testing process. Full test coverage ensures holistic assessment of device compliance. Regular calibration and validation ensure accuracy and reliability. Realistic test scenarios simulate real-world operating conditions and environmental variables. Collaboration fosters knowledge-sharing and problem solving between cross-functional teams. Continuous improvement builds on the feedback from pre-conformance testing to refine product design and optimize compliance.

2.7.3 Expected impact

In today's interconnected world, C&I are critical to business success. They enable companies to create a portfolio of intelligent products, ensuring seamless product integration and complementarity. This creates a cohesive ecosystem that improves user experience and customer satisfaction. Integrating C&I into product development processes from the outset helps address compatibility issues, streamline integration efforts, and accelerate time-to-market. This approach reduces the risk of costly redesigns or upgrades later in the product lifecycle.

Understanding the human and material resources required for C&I testing is crucial for effectively planning and executing tests. Assigning the right expertise, infrastructure and support minimizes delays, reduces costs and optimizes resource utilization.

Regulators can support emerging products and industries by advocating for the establishment of MRAs between administrations, which simplify regulatory compliance by recognizing conformity assessment results across jurisdictions or sectors. This facilitates market access for innovative products and promotes global collaboration.

Regulators can also promote informed dialogue with entrepreneurs by providing advice, resources and educational initiatives. This fosters trust, transparency and collaboration between regulators and entrepreneurs, leading to better regulatory outcomes and an environment conducive to innovation and business growth. Overall, C&I are critical to the success of businesses in today's interconnected world.

Chapter 3 – Combating the illegal use of devices: counterfeiting, quality defects and theft of mobile devices

3.1 The challenge of the proliferation of counterfeit devices

The proliferation of counterfeit and substandard devices is a growing problem for consumers, legitimate industries, governments and international organizations. Counterfeit devices are often manufactured without meeting safety and quality standards and pose a potential threat to national digital transformation programmes in developing countries. In addition to compromising security, network performance and quality of service, counterfeit devices expose the public to multiple health and environmental risks. The economic impact of counterfeit electronic equipment can also reduce the contribution of a country's ICTs sector to GDP.

The fight against counterfeit devices requires multi-pronged approaches with guidelines that enable governments, businesses and international organizations to work together to reduce the proliferation of counterfeit devices and improve the safety and quality of electronic products in countries.

This chapter includes definitions and guidelines to combat the influx of counterfeit and substandard devices, with a focus on national experiences (case studies).

The main objective of combining the different approaches discussed in this chapter is to create an environment where consumers have access to authentic and quality electronic products, while reducing the risks associated with counterfeiting and the manufacture of substandard counterfeit products.

Combating the proliferation of counterfeit and substandard devices:

- Aims to protect consumers from the potential hazards associated with the use of these products, such as health, safety and performance risks, as well as to preserve the integrity of legal industries and the reputation of legitimate brands.

Efforts to counter this proliferation may include:

- The promotion of certification and traceability for electronic products;
- Cooperation between governments, industry and international organizations.

3.2 Guidelines

Guidelines should be developed to better combat the proliferation of counterfeit and substandard devices in developing countries, including:

- **Certification and traceability:** establish certification and traceability programmes for legitimate electronic products to make it harder to tamper with them and to distribute counterfeit products;

- **Public-private partnerships:** encourage collaboration with authorized manufacturers, trade associations and international organizations to identify and eliminate supply chains for counterfeit products;
- **Regional and international collaboration:** encourage collaboration with other countries and international organizations to share information and good practices in combating counterfeiting;
- **Training and capacity building:** invest in training and capacity building for law enforcement agencies to improve their effectiveness in combating counterfeiting;
- **Promote reporting mechanisms:** establish mechanisms for consumers to report counterfeit products and encourage competent authorities to investigate and take action;
- **Corporate social responsibility:** encourage companies to adopt responsible business practices by committing to not using counterfeit products in their supply chain and by contributing to awareness and training programs.

3.3 Theft of mobile devices

Mobile device theft is a global problem that affects both individuals and businesses. With the proliferation of smartphones, laptops, tablets and other handheld devices, their attractiveness to criminals has increased dramatically. These devices often contain sensitive information, such as personal, banking and business data, making them prime targets for not only physical theft but digital attacks as well. The fight against this scourge requires a holistic approach that integrates technical, legislative, and public awareness-raising measures.

Mobile phone theft statistics[9]

Mobile phone theft is a global phenomenon that is constantly increasing, affecting both individuals and businesses.

According to various studies and reports:

- Every year, approximately 70 million smartphones are stolen or lost worldwide.
- Around 10 per cent of mobile phone users will be the victim of theft or loss during the lifetime of their device.
- In some major cities, smartphone thefts account for up to 50 per cent of reported crimes.
- Only 7 to 10 per cent of stolen devices are recovered by their owners.
- Around 40 per cent of phone thefts occur on public transport or in busy public places.

These figures show the scale of the problem and highlight the importance of prevention and protection measures.

Security and privacy impact

Mobile phone theft is a concern not only because of the physical loss of the device: it also poses a critical threat to the security and privacy of personal and business data. Thieves can exploit personal, banking, and business information stored on the device.

[9] GSMA. Mobile Device Theft - State of Affairs Report. February 2025.

The security impacts of unauthorized access to sensitive data include:

- Risk of cyberattacks and fraud: criminals can use the phone to access online accounts, make fraudulent purchases or impersonate the owner.
- Exposure of corporate data: in a business setting, a stolen phone can provide access to confidential data, compromising an organization's cybersecurity.
- Criminal use: some stolen phones are used for illegal activities, such as phone fraud or cybercrime.
- Disclosure of personal information: stored photos, videos, messages and documents can be exploited for malicious purposes.
- Privacy invasion: social media and messaging apps can be compromised, leading to identity theft and breach of private communications.
- Sale of data on the black market: information contained in a phone can be resold on the dark web, jeopardizing the user's digital security.

Mitigation measures

To minimize the risks associated with mobile phone theft, several strategies can be implemented:

- Prevention and protection through the use of security locks: activating PIN codes, strong passwords and biometric authentication (fingerprint, facial recognition).
- Data encryption: protecting sensitive files prevents their exploitation in the event of theft.
- User awareness: learning good security practices, such as avoiding exposing your phone in risky places.
- Increased surveillance: making sure to never leave your phone unattended, especially on public transport and in public spaces.
- Remote tracking and wiping in response to theft: using services such as Find My iPhone (Apple) or Find My Device (Android) to find, lock or erase data remotely.
- IMEI blocking: reporting the theft to the mobile operator to deactivate the device and make it unusable on the network.
- Complaint filing: reporting the theft to the authorities to try to recover the device and prevent possible fraudulent use.
- Immediate password change: changing the login credentials of applications and services linked to the phone to prevent unauthorized access.
- Regulatory and technological measures for operators to block stolen devices: establishing international databases to prevent the activation of stolen phones.
- Requirement for manufacturers to integrate anti-theft solutions: implementing features such as automatic data erasure after several unsuccessful login attempts.
- Strengthened legislation: adopting laws to punish acquiring and reselling stolen devices.

3.4 Problems and issues

- **Loss of sensitive data:** when mobile devices are stolen, users are at risk of losing critical personal and business information, which can lead to privacy breaches.
- **Identity theft:** data stored on stolen devices can be exploited for fraudulent or identity theft activities.
- **Service inaccessibility:** the theft of a device can cut off the user's access to essential services, thus affecting their daily activities.

- **Black market resale:** stolen devices are often resold on a global black market that evades regulation and exacerbates the crime problem.
- **Lack of standardization in legislative responses:** laws and sanctions vary from country to country, making it difficult to have a coordinated response at the international level.
- **Device recovery efforts:** current traceability devices do not always guarantee the recovery of stolen devices.
- **Roles of telecom operators:** operators have a key role to play in blocking access to networks for stolen devices, but the measures applied differ by region.
- **User awareness and education:** campaigns to raise public awareness about the risks of mobile device theft and good digital security practices, such as enabling device lockout and traceability mechanisms, are crucial.
- **Strengthen legislation:** governments must put in place strong laws to deter the theft of mobile devices, harmonize penalties internationally, and work with operators and manufacturers to prevent the use of stolen devices.
- **Traceability technology:** the widespread adoption of remote device tracking and locking technologies should be encouraged. Manufacturers should also incorporate more robust anti-theft measures into their products.
- **Involvement of telecom operators:** operators must put in place mechanisms to quickly block stolen devices and make it more difficult for them to be used on other networks. They should also participate actively in international databases of stolen devices.
- **International coordination:** efforts to combat mobile device theft need to be strengthened at the international level, with the creation of centralized databases to track stolen devices and mechanisms for sharing information between countries.

By implementing these guidelines, governments, businesses and international organizations can work together to reduce the proliferation of counterfeit devices and improve the safety and quality of electronic products in countries, especially developing countries.

3.5 Country case studies

The contributions of Member States and stakeholders have played a fundamental role in the development of this report. Based on national experience, available data and existing practices, these contributions aim to effectively combat the proliferation of counterfeit devices.

All contributors agreed on the importance of establishing appropriate policy, legal and regulatory frameworks to address this challenge.

Furthermore, some suggested adopting proven technical solutions, including the implementation of international standards, the use of market surveillance techniques, and the creation of databases and centralized platforms to block counterfeit devices.

Particular emphasis was placed on the need to support developing countries in implementing C&I programmes while strengthening efforts to combat the counterfeiting of ICT equipment and the theft of mobile devices.

Additionally, several contributors recommended intensifying efforts at the regional and sub-regional levels to pool various approaches and techniques, enabling a more effective fight against device counterfeiting.

3.5.1 Republic of Zambia

A document from Zambia was presented on the proliferation of counterfeit and altered mobile phones, which poses a major threat to the digital transformation programmes of developing countries, and Zambia in particular. These devices not only compromise security, network performance and service quality, but also expose populations to health risks and reduce the ICT sector's contribution to GDP.

Identified challenges

- Lack of regional collaboration in the fight against counterfeiting.
- Absence of baseline data to guide national and regional strategies.
- Financial accessibility issues for authentic mobile phones.
- Low consumer awareness of the risks associated with counterfeit devices.

Case of Zambia

- Zambia is surrounded by eight neighbouring countries and is experiencing a growing demand for mobile phones, and is therefore particularly vulnerable to the influx of counterfeit devices.
- The government has implemented measures such as:
  - the adoption of electronic communications laws;
  - type approval of ICT devices;
  - collaboration between ICT authorities and immigration, customs, and tax authorities;
  - the development of the Integrated Electronic Communication Equipment Registration System (IECERS).

Ongoing initiatives

- Zambia is exploring the use of the IMEI verification service of the GSM Association to enable consumers to verify the authenticity of devices before purchase.
- This initiative aims to reduce the demand for counterfeit devices and raise consumer awareness.

Recommendations

- Regional solutions: encourage a collaborative approach among Member States to combat the trade in counterfeit phones.
- Training and projects: develop national and regional programmes to strengthen government capacities.
- Regional reports: publish data on the volumes and trends of counterfeiting to better inform consumers.
- Regional platform: create a rapid reporting system for stolen devices to protect consumers.

Conclusion

The fight against counterfeit phones requires a comprehensive approach, combining technical solutions, regional collaboration and increased consumer awareness. Zambia, through its

initiatives and the adoption of technologies such as the IMEI service of GSMA, is paving the way for other developing countries to follow.[10]

3.5.2 Guinea

Introduction

With the rapid evolution of technologies and the emergence of new mobile devices, applications and services, citizens are increasingly reliant on ICTs, often without being aware of the risks involved. It is essential for States to establish coherent national policies to protect their citizens.

Background

In Guinea, citizens are frequently victims of mobile device theft, cyberattacks and fraudulent activities. Measures taken by the authorities include:

- The adoption of Law 2016/037/AN on cybersecurity and the protection of personal data.
- The creation of the National Agency for Information Systems Security (ANSSI).
- A feasibility study for the establishment of a national computer emergency response team (CERT) and security operations centre (SOC).

Nevertheless, citizens remain vulnerable in the event of loss or theft of their devices, facing difficulties in recovering their data or restoring their SIM cards. Counterfeit devices flood the market, exacerbating issues of fraud and service quality.

Fight against fraud

A monitoring committee, coordinated by the Regulatory Authority for Posts and Telecommunications of Guinea (ARPT), has been established to combat unauthorized and counterfeit devices. Actions taken include:

- A campaign for the certification of imported devices.
- The detection and disconnection of 1 000 fraudulent numbers in 2023.
- The dismantling of six SIMBOX sites in Conakry.

Fight against device theft

ANSSI and ARPT collaborate to track thieves and stolen devices. A centralized mobile device identification and SIM card registration platform has been set up to manage mobile terminals and identify those that are non-compliant, cloned or stolen.

Conclusion

To effectively combat this scourge, the following measures are proposed:

- Establishment of a harmonized national strategy to combat device theft, counterfeiting and cyberattacks.
- Sharing of experiences and good practices among ITU Member States.

[10] ITU-D SG2 Document SG2RGQ/37 from Zambia.

- Support from ITU to help developing countries develop common strategies and operationalize their national CERTs.

Key points

- Guinean citizens are exposed to risks related to device theft, counterfeiting and cyberattacks.
- Measures have been taken, including the creation of ANSSI and the establishment of detection and device management platforms.
- Regional and international collaboration is essential to strengthen the fight against these issues.[11]

3.5.3 Republic of Chad

In Chad, the reduction of the digital divide has led to a significant increase in the number of mobile phone users and Internet users. However, this expansion comes with major challenges, including the proliferation of counterfeit or falsified phones, as well as a rise in device theft. These issues compromise user security, the quality of telecommunications services, and network performance.

The Chadian Government, through the Ministry of Telecommunications and the Digital Economy, has implemented measures to modernize infrastructure and reduce the digital divide. However, the market is flooded with unverified devices, often imported without any checks, exposing users to security and quality risks. The Regulatory Authority for Electronic Communications and Posts of Chad (ARCEP) plays a key role in regulating the sector but lacks the technical means to effectively verify devices and combat theft and counterfeiting.

To address these challenges, several recommendations are proposed, including:

- Establishing a certification laboratory compliant with GSMA standards.
- Strengthening collaboration between ARCEP, customs authorities and operators to verify devices before they enter the market.
- Launching awareness campaigns to inform consumers about the risks associated with counterfeit or stolen devices.
- Establishing regional agreements to facilitate the tracking of stolen devices and cooperation between countries.

In conclusion, although efforts have been made, the fight against phone theft and counterfeiting in Chad is still in an early stage. A coordinated approach, including technical, regulatory and regional measures, is essential to protect users and improve the quality of telecommunications services.[12]

3.5.4 Sri Lanka

The Telecommunications Regulatory Commission of Sri Lanka (TRCSL) regulates mobile device imports under the Sri Lanka Telecommunication Act No. 25 of 1991. Licensed operators must maintain an equipment identity register (EIR) to ensure only legally imported, IMEI-enabled devices are activated. TRCSL mandates type approval for telecommunication devices and

[11] ITU-D SG2 Document SG2RGQ/115 from Guinea.
[12] ITU-D SG2 Document SG2RGQ/112 from Chad.

maintains an IMEI database for legally imported devices. Fines for non-compliance were recently increased significantly. An online system now allows the public to report lost or stolen phones, improving efficiency and reducing costs. TRCSL also operates an IMEI verification system for customers to authenticate devices via SMS, though enforcement against illegal imports faces challenges.[13]

3.5.5 Rwanda

Over the last two decades, the ICT sector, including mobile technology, in Rwanda has advanced significantly, which has led to an expanded market for mobile devices. However, this growth has also resulted in a significant proliferation of counterfeit mobile devices. If the issue is not properly managed, it may pose security threats, hinder economic growth, cause operational risks and negatively impact user trust. To address these issues, Rwanda has implemented tools, legal frameworks and institutional collaborations to combat counterfeit and stolen devices, aligning with ITU recommendations. Key stakeholders such as customs authorities, consumer protection agencies, telecom operators, and security entities work together to ensure only legal devices are used. Public reluctance and low awareness about data protection remain hurdles. Joint awareness campaigns and inter-agency collaboration have demonstrated strong potential.[14]

[13] ITU-D SG2 Document 2/367 from Sri Lanka.
[14] ITU-D SG2 Document 2/352 from Rwanda.

Chapter 4 - Conformance and interoperability for the Internet of Things

4.1 Introduction

IoT is a global infrastructure for the information society, enabling advanced services by interconnecting physical and virtual things based on existing and evolving interoperable ICTs.[15]

IoT technologies can be found in many industries and affect the daily lives of IoT individuals through platforms that process data from billions of connected devices. A study by IoT Analytics shows that there are 16.7 billion active IoT endpoints, and it is predicted that there will be more than 29 billion IoT connections by 2027.[16]

4.2 IoT ecosystem and application scenarios

4.2.1 IoT ecosystem

IoT is the network of physical things or devices equipped with electronic components, software, sensors and network connectivity that enable them to collect and exchange data. These devices collect useful data using various existing technologies and autonomously circulate data between other devices. Stakeholders are concerned about the security and reliability of the connections and devices, and the privacy of the stored and transmitted data. The IoT ecosystem includes:

- **Devices and sensors**: the core elements of IoT, these are physical objects equipped with sensors and actuators that collect data from their environment or perform specific actions based on the instructions received. Examples include temperature sensors, motion sensors, wearable devices and smart meters.
- **Connectivity**: it provides devices with the means to communicate with each other and with core or cloud-based systems where additional processing is done. The technologies used include Wi-Fi, Bluetooth, cellular (LTE, 5G), and low-power wide area network (LPWAN) (long range wide area network (LoRaWAN), Sigfox).
- **Data processing equipment**: it processes the data collected by sensors before it is sent to the cloud or to local servers for more intensive computation. Implementation includes edge computing devices that pre-process data to reduce latency and bandwidth usage.
- **Platform**: it acts as the backbone of the IoT system, integrating different devices, managing their communications and enabling the flow of data between them. Its capabilities include device management, data collection and app activation.
- **Cloud servers & data centres**: they provide the infrastructure needed to store large amounts of IoT data and run complex analytical models to extract actionable insights. They are often integrated with AI and machine learning capabilities for advanced predictive analytics.

---

[15] Recommendation ITU-T Y.4000/Y.2060 (06/2012). Overview of the Internet of Things (IoT).
[16] IoT Analytics. State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally. 3 September 2024.

- **User interface**: it includes dashboards, mobile apps, and other user interfaces that allow users to interact with the IoT system, configure settings, and view data in an understandable format. It can be tailored to meet specific needs, providing relevant information and controls to the user.
- **Security**: it aims to protect the integrity and confidentiality of IoT data and systems from cyberthreats. Metrics includes encryption, two-factor authentication, secure boot, and regular security updates.
- **Standards & regulation**: standardization ensures the interoperability and compatibility of devices. It adheres to regional and international regulations governing data protection, privacy, the free flow of data across borders, and device operation across different industries.

4.2.2 Application scenarios

Many new IoT applications have emerged in recent years. The most relevant and active application scenarios are as follows:

- Smart automation of home environments through connected devices such as thermostats, lights and security systems, that can be controlled and monitored remotely;
- Remote patient monitoring systems, wearable health devices, and telemedicine solutions that improve patient care and health management;
- Precision farming techniques that use sensors to measure soil moisture, weather conditions and crop health, improving yields and resource efficiency;
- Smart factories that are equipped with sensors and automated machinery to increase production efficiency, predictive maintenance and supply chain optimization;
- Transport and logistics fleet management solutions, real-time vehicle tracking and intelligent traffic management systems that optimize logistics and reduce congestion;
- Smart inventory management systems, new in-store ICT devices, and personalized marketing that enhance retail services and improve the customer experience;
- Smart cities that integrate the management systems of city services such as traffic, waste management and energy consumption to improve sustainability and urban life;
- Smart grids and new ICTs devices that improve energy efficiency and management in homes, buildings and cities.

4.2.3 Classification of IoT devices

IoT devices are classified into three categories based on their computing power and communication capabilities:[17]

- low processing and low connectivity (LPLC) devices;
- low processing and high connectivity (LPHC) devices;
- high processing and high connectivity (HPHC) devices.

Recommendation ITU-T Y.4108 covers devices such as tags without processing power.

[17] Recommendation ITU-T Y.4460 (06/2019). Architectural reference models of devices for Internet of Things applications.

HPHC device functional entities

Sensing/actuation/data capture functional entity; messaging functional entity; gateway access functional entity; materiel management functional entity; functional entity that interfaces with cloud services/applications; connectivity management functional entity; application execution engine functional entity; device management functional entity; information-sharing functional entity; data analysis functional entity; data storage functional entity.

LPHC device functional entities

Sensing/actuation/data capture functional entity; messaging functional entity; gateway access functional entity; materiel management functional entity; functional entity that interfaces with cloud services/applications; connectivity management functional entity.

LPLC device functional entities

Sensing/actuation/data capture functional entity; LPLC message processing functional entity; gateway access functional entity; and materiel management functional entity.

The ISO/IEC Joint Technical Committee 1 (JTC1) Report on IoT provides general information on the subject, including examples of the drivers, regulation, security, privacy and governance of IoT technology.

4.3 IoT challenges related to C&I

Some of the issues and challenges related to meeting the specific needs of IoT, such as quality, reliability, coverage and low power consumption, were addressed in the final report of ITU-D Question 4/2 (study period 2018-2021).[18] In recent years, new trends have been emerging and gaining momentum, which increase the complexity of IoT platforms and protocols. The IoT certification scheme must undergo regular review to ensure alignment with the latest developments. More factors need to be considered during the technical selection and the deployment of IoT devices and systems.

Increasing share of satellite connectivity

As satellite launch costs decrease, connectivity via low-Earth orbit (LEO) satellites is becoming increasingly popular. Connectivity via LEO satellite has lower path loss and therefore requires less terminal power and less antenna directivity, making it easier and cheaper to design and deploy IoT devices. Research shows that the satellite IoT market will continue to become increasingly competitive and the market size should reach USD 1 billion. However, the sweet spot for satellite IoT connectivity remains its deployment in remote and isolated areas. The total size of the satellite IoT market will remain a fraction of the entire IoT market for the foreseeable future.

[18] ITU-D. Final Report on ITU-D Study Group 2 Question 4/2 for the study period 2018-2021. Assistance to developing countries for implementing conformance and interoperability programmes and combating counterfeit ICT equipment and theft of mobile devices. ITU, 2021.

Convergence of AI and IoT

It is estimated that nearly half of all IoT applications will be AI-enabled by 2027.[19] The integration of AI into IoT applications will see strong growth and is expected to increase sharply in the coming years.

The convergence of AI and IoT, known as AIoT, is developing rapidly with the large-scale application of AI technology. AI technology can provide more accurate data analysis and processing capabilities for IoT applications, helping users better manage and control IoT devices. IoT devices provide AI with more sources of data and applications, enabling it to better understand the environment, recognize patterns and improve decision-making in various domains.

For example, the convergence of AI and IoT brings more opportunities for smart homes. AI can monitor the home environment in real-time and intelligently regulate it by connecting different home devices. In smart city scenarios, AI can collect real-time information about the city and support smart planning and decision-making by connecting various infrastructures and devices in the city. The transportation system can adjust traffic lights in real-time and optimize traffic flow through AI algorithms.

4.4 Regulation and policies for IoT products

IoT, by its very nature, requires that regulatory frameworks and governance policies adapt in order to manage the new dynamics it introduces to the ICT sector. Here are some key aspects to consider:

- **International interoperability standards**: several organizations, including ITU, ISO and IEEE, are working to develop global standards governing the interoperability of IoT devices. These standards aim to ensure technical harmonization, facilitating the large-scale deployment of IoT solutions.
- **IoT security regulations**: faced with the proliferation of connected objects, harmonized regulations are necessary to ensure the security of these devices. Governments are putting laws in place that require manufacturers to adhere to minimum security protocols in order to protect ICTs network from malicious intrusions.
- **Data protection policies**: with the increase in data generated by IoT, regulatory authorities are imposing strict data protection obligations, such as the GDPR in Europe. These laws require IoT enterprises to ensure the privacy and security of personal information collected through their devices.
- **Certification initiatives:** to ensure that IoT products meet C&I standards, some jurisdictions encourage or require certification processes. Such certifications can cover both technical compatibility and aspects related to consumer protection and environmental sustainability.

The regulatory framework for IoT is a set of policies, standards and guidelines designed to oversee the development, deployment and management of IoT technologies. An effective regulatory framework is essential to ensure the security, privacy, interoperability and ethical use of IoT devices and data.

The regulatory framework for new ICTs must provide for:

- The development of security standards;

[19] https://iot-analytics.com/how-enterprise-iot-market-is-evolving/

- The protection of privacy;
- The development of interoperability requirements;
- The development of quality of service and reliability standards;
- Consumer protection laws;
- Compliance with international standards;
- The development of ethical guidelines.

Firstly, the local regulator should provide:

- Device and network certification;
- Spectrum management;
- Data governance and sovereignty.

Device certifications ensure that devices meet regulatory standards before they are placed on the market. Network certifications are mandatory and ensure that IoT devices operate safely within the network infrastructure.

Spectrum management regulates the use of radio frequencies to avoid interference and ensure reliable communication for IoT devices.

Data governance defines the rules for the ownership, sharing and transfer of data, especially in cross-border operations. Data sovereignty standards determine how data is stored, processed and protected.

4.5 Compliance standards for new IoT devices

Standards development organizations around the world are committed to establishing comprehensive frameworks for new ICT devices to ensure their safety, interoperability and effectiveness. These standards form part of a concerted effort by these organizations to provide clear guidance on the development and implementation of new ICTs. They cover a variety of aspects, including requirements for the physical, network, session, and application layers, and security and confidentiality considerations. Standards development organizations such as ITU, IEEE and ISO are actively working to develop and maintain standards to ensure the compliance of new ICT devices.

ITU provides the following standards: ITU-T Y.4000/Y.2060 (06/2012) – Overview of the Internet of Things;[20] and ITU-T Y.4100/Y.2066 (06/2014) – Common requirements of the Internet of things.[21]

ISO and IEC provide the following standards: ISO/IEC 30141 (2024): Internet of Things (IoT) – Reference architecture;[22] and ISO/IEC 27400 (2022): Cybersecurity – IoT security and privacy – Guidelines.[23]

ETSI provides the following: technical specification ETSI TS 103 645 (01/2024) Cyber Security for Consumer Internet of Things: Baseline Requirements, which provides a high-level guide to

[20] Recommendation ITU-T Y.4000/Y.2060 (06/2012) Overview of the Internet of Things.
[21] Recommendation ITU-T Y.4100/Y.2066 (06/2014) Common requirements of the Internet of things.
[22] ISO/IEC 30141 (2024) Internet of Things (IoT) – Reference architecture.
[23] ISO/IEC 27400 (2022) Cybersecurity – IoT security and privacy – Guidelines.

consumer IoT security;[24] and European standard ETSI EN 303 645 (09/2024) Cyber Security for Consumer Internet of Things: Baseline Requirements, which establishes cybersecurity standards for consumer IoT devices to protect users' privacy and personal data.[25]

The American National Standards Institute (ANSI) and the Telecommunications Industry Association (TIA) provide the following standards: ANSI/TIA-942-C (07/2024) Telecommunications Infrastructure Standard for Data Centers, which specifies telecommunications infrastructure standards for data centres, with considerations for IoT deployments;[26] and ANSI/TIA-1179-B (06/2023) Healthcare Facility Telecommunications Infrastructure Standard, which establishes standards for telecommunication infrastructure in health-care facilities that support IoT devices.[27]

3GPP provides the following standards: TS 22.368 (04/2025) Service requirements for Machine-Type Communications (MTC), which includes IoT aspects;[28] and TS 23.682 (03/2025) Architecture enhancements to facilitate communications with packet data networks and applications, which describes architecture enhancements to facilitate IoT and machine-to-machine (M2M) communications.[29]

OneM2M provides the technical specifications for a common M2M service layer that can be integrated into hardware and software to connect devices. OneM2M also provides TS-0004 Service Layer Core Protocol, which specifies the communication protocol(s) for oneM2M compatible systems, M2M applications and/or other M2M systems.[30]

Special working group 5 (SWG 5) of the ISO/IEC JTC1 was responsible for studying IoT and related technologies, including smart grid, and exchanging information to facilitate coordination. It was disbanded in 2014, its work being continued by working group 10 of ISO/IEC JTC 1 until 2016, when subcommittee 41 of ISO/IEC JTC1 inherited the latter's programme of work.

Specific technical reporting and activities provide the following standards: Efforts to ensure that IoT devices are compliant with existing X73 standards in health care, specifically personal health devices (IEEE 11073 standards). Benchmarking of ISO/IEC and IEEE standards in the field of IoT to ensure C&I between devices and systems from different manufacturers.

One use case is the experimentation of a wireless sensor network (WSN) consisting of IoT devices communicating with each other using a wireless protocol. The objective of the experimentation is to evaluate the performance of these IoT devices in real conditions and in different environments. Multiple testbeds should be used, with each one representing a specific environment where the wireless IoT devices are installed. The testbed infrastructure is accessed remotely to prepare and control the wireless IoT experiment. Typical parameters to be measured in such a wireless network are reliability, latency, radio duty cycle, number of hops, synchronization and bandwidth. This experiment requires the following conditions:

- Relevance: the tests and parameters to be measured must be relevant to the real conditions encountered in an industrial deployment.

---

[24] ETSI TS 103 645 Cyber Security for Consumer Internet of Things: Baseline Requirements.
[25] ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements.
[26] ANSI/TIA-942-C Telecommunications Infrastructure Standard for Data Centers.
[27] ANSI/TIA-1179-B Healthcare Facility Telecommunications Infrastructure Standard.
[28] 3GPP 22.368 Service requirements for Machine-Type Communications (MTC)
[29] 3GPP 23.682 Architecture enhancements to facilitate communications with packet data networks and applications
[30] OneM2M TS-0004 Service Layer Core Protocol.

- Reproducibility: the experiment must be redone on different test benches and under different conditions.
- Repeatability: the experiment must be repeated under the same conditions.
- Automation: the experiment must be run automatically.

A testbed federation such as Fed4FIRE+ provides all the tools and services needed to meet these requirements, enabling the experiment to be run and repeated under the predefined conditions.

Chapter 5 – Knowledge transfer

5.1 Introduction

In order to successfully transfer C&I knowledge and expertise, it is essential to assess existing competencies, identify knowledge gaps and, most importantly, provide effective and appropriate training.

5.2 C&I training needs and opportunities

The Dubai Action Plan (WTDC-14) recalls that widespread conformance and interoperability of telecommunication/ICT equipment and systems increases market opportunities, improves reliability and simplifies integration and international trade.

However, this generalization highlights disparities and problems in the acquisition and ownership of compliance processes or processes that need to be assessed to achieve objectives.

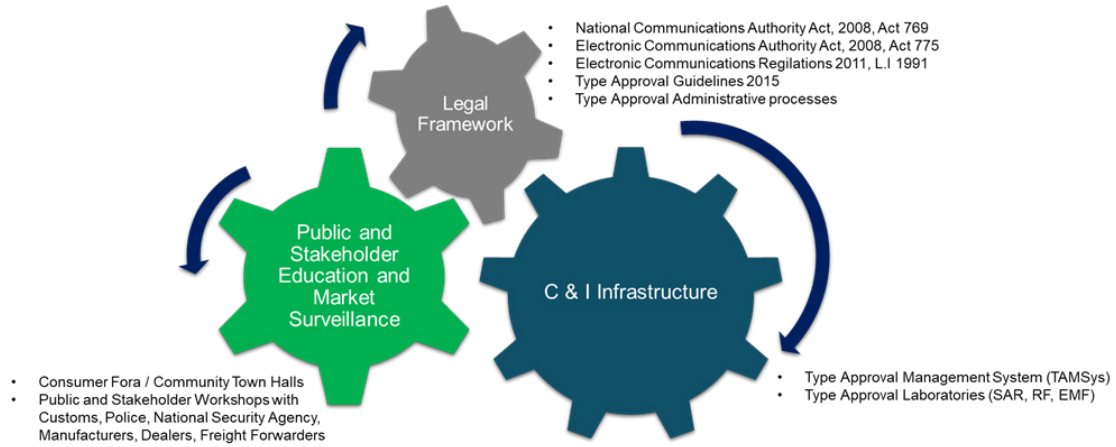
The impact of issues related to conformance, interoperability or underperformance of ICT equipment is multidimensional. User security, certification of technicians, the standardization of design processes at the manufacturer level, support for government decision-making, and the quality of network services must be taken into account in establishing an effective knowledge-transfer framework.

The continuous innovations and developments concerning digital technologies have revealed the need to train and educate compliance stakeholders in order to ensure compliance with regulatory requirements and prevent the risks associated with non-compliance.

In addition to the challenges of mastering innovative technological equipment, understanding and formulating the legal framework, acquiring and implementing C&I infrastructure, and monitoring contracts, there are other challenges that could be solved by a specific training and knowledge-transfer programme.

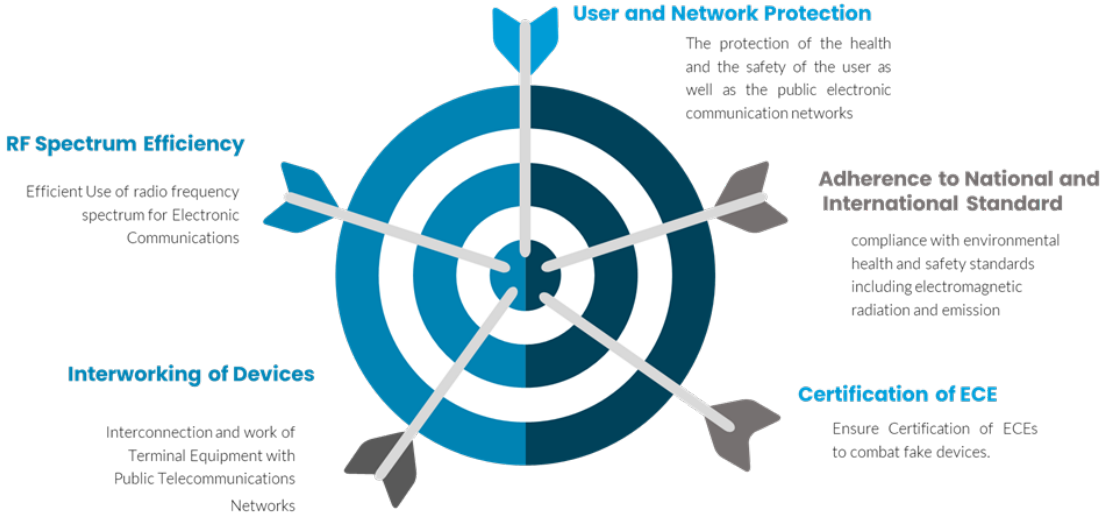
The National Communications Authority (NCA) of Ghana described the purpose, challenges, indicators, components, technical standards, specifications and requirements, regulatory requirements, and infrastructure of its C&I regime for combating counterfeit ICT devices through C&I testing and market surveillance.

Figure 3: Composition of the C&I regime in Ghana



Source: Ghana[31]

Figure 4: Objectives of the C&I regime in Ghana



Source: Ghana[32]

As a follow-up to this case study from Ghana, Republic of Kenya, in collaboration with the DiploFoundation, provided an example of a regulatory framework for conformity assessment activities in Africa.

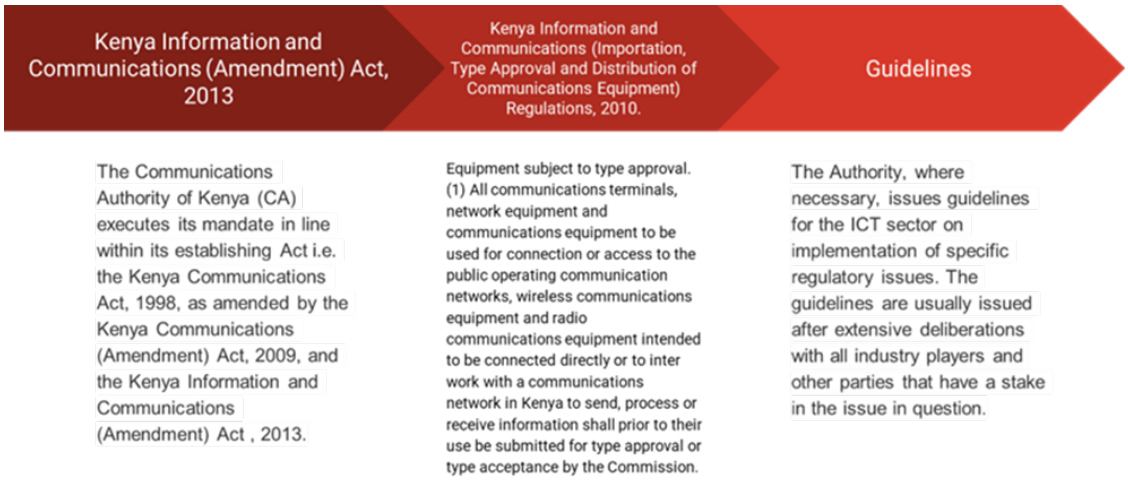
The framework builds on the activities of the Kenya Bureau of Standards (KEBS), the national standards body responsible for developing and implementing standards and conformity assessment procedures in the country, as well as the ICT regulator of Kenya, the Communications Authority.

---

31 Roland Yaw Kudozia. Ghana. Combating counterfeit ICT devices through C&I testing and market surveillance. ITU-D Workshop on conformance and interoperability challenges for digital transformation, Geneva, 2 June 2023.

32 *Ibid*.

Figure 5: Objectives of the C&I regime in Kenya



Source: DiploFoundation[33]

5.3 Responses to knowledge acquisition and retention needs

In line with the Buenos Aires Declaration adopted by WTDC-17, widespread C&I of telecommunication/ICT equipment and systems through the implementation of relevant programmes, policies and decisions can increase market opportunities, reliability and promote global integration and trade.

Therefore, Member States and ITU-D Sector Members are encouraged to assist and guide one another by studying, identifying ways to bridge the standardization gap, and addressing issues related to issues raised in WTDC Resolution 47 (Rev. Kigali, 2022), Resolutions 44 and 76 (Rev. New Delhi, 2024) of the World Telecommunication Standardization Assembly (WTSA), and Resolution 177 (Rev. Bucharest, 2022) of the Plenipotentiary Conference.

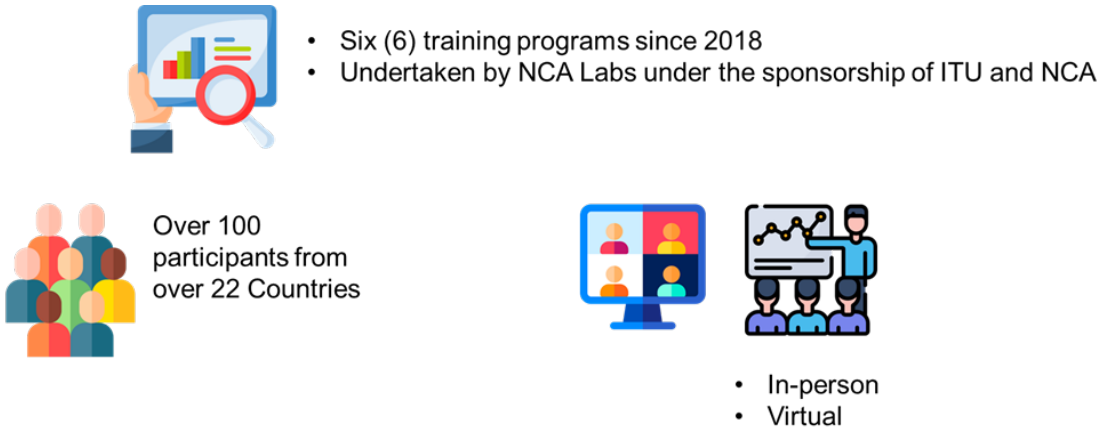
To respond to this need for collaboration and to assist the international community in achieving the SDGs, several initiatives have been undertaken to develop C&I competencies. These initiatives, carried out in collaboration with ITU, have been reported on by BDT.

These contributions present experiences in capacity building in the Africa region and also inform the ITU membership about the future digital networks and infrastructure (including activities, actions, events and/or resources such as trainings and guidelines) that have been developed.

Since 2018, six C&I training programmes have been organized for Africa by the NCA Labs of Ghana and were sponsored by ITU, through the ITU Academy, and NCA.

[33] Mwende Njiraini. DiploFoundation. Conformance and interoperability assessment in Africa: case study of Kenya. ITU-D Workshop on conformance and interoperability challenges for digital transformation, Geneva, 2 June 2023.

Figure 6: ITU-NCA training for Africa



Source: Ghana[34]

This sharing of experience has made it possible to respond to specific compliance issues related to:

- Regulatory and legal aspects, including MRAs and EMC.
- Problems encountered in acquiring basic C&I infrastructure to facilitate type approval and market surveillance.
- The need for technical cooperation among participants.
- Difficulties in interpreting test reports of different items of telecommunication equipment, etc.

The Egyptian African Telecom Regulatory Training Centre (EG-ATRC), launched by Egypt in July 2021, aims to enhance the skills of African professionals in the ICT sector to promote a digital Africa. The ITU-accredited centre provides both theoretical and practical training through in-person and online sessions. The training courses cover areas such as cybersecurity, smart cities and the certification processes for communication equipment to ensure compliance with international standards. Over 50 countries have participated, with 381 individuals trained so far. The centre's programmes facilitate knowledge transfer to African regulators and contribute to the development of digital strategies and regulatory frameworks across the continent.[35]

In addition to the national initiatives of Member States, which are real levers for the transfer of experience and knowledge, ITU provides members with information on the work of the Telecommunication Development Bureau (BDT) in the field of ICT infrastructure and also resources that have been or are being developed to facilitate the adoption of ICT infrastructure policies and strategies in various countries and regions.

This ITU support to Member States accelerates connectivity, leverages local, national and regional knowledge, and contributes to the common goal of building inclusive digital societies worldwide. These resources cover various topics such as ICT networks (ICT infrastructure mapping and geospatial analysis, ICT business planning toolkit, IMT 2020/5G), emerging

[34] Roland Yaw Kudozia. Ghana. Combating counterfeit ICT devices through C&I testing and market surveillance. ITU-D Workshop on conformance and interoperability challenges for digital transformation, Geneva, 2 June 2023.
[35] ITU-D SG2 Document 2/329 from Egypt.

technologies, technical assistance to Member States, training opportunities (IPV6, IoT, 5G, exchange points...), C&I, last mile connectivity, and exposure to electromagnetic fields.[36]

With regard to C&I, the ITU Academy organized a training course for the African region on conformity and interoperability on test reports analysis and regulatory aspect of EMC testing.

5.4 Guidelines for developing conformance and interoperability programmes

In conclusion, the various development objectives can be achieved by implementing programmes that ensure widespread C&I of telecommunication/ICT equipment and systems, and which combine the real needs and capabilities of developing and least developed countries.

However, in order to develop such programmes, these guidelines must be followed:

- Provide an up-to-date overview of current C&I situations in developing and least developed countries in order to effectively address challenges and align responses with real needs.
- Make relevant information from ITU and other standard organizations available to Member States in order to raise awareness of the benefits of compliance.
- Improve the classification and segmentation of training courses to better meet the needs of beginners and specialists.
- Develop and refine training modules to improve the skills of each individual.

[36] ITU-D SG2 Documents 2/48, 2/189, 2/253, SG2RGQ/49 and SG2RGQ/194 from ITU BDT.

Chapter 6 – Conformance and interoperability issues: challenges, solutions and prospects

6.1 New technologies beyond regulatory/testing procedures

Development beyond regulatory procedures and testing requires a single mechanism to achieve the best results in the shortest time frame.

The plan, do, check, act (PDCA) cycle is a continuous improvement cycle, also called the Deming cycle or Deming wheel. It is a structured method for solving problems, improving processes or optimizing projects. Such an approach will unify the development procedures beyond the regulatory and testing procedures and ensure their effectiveness, integrity and adequacy.

Reducing time-to-market and the gradual implementation of rules and procedures for new technologies

- Step 1: Use of test protocols available from equipment manufacturers in conjunction with the analysis procedure.
- Step 2: Deployment of the test area for compatibility testing.
- Step 3: Development of established requirements and testing in an accredited laboratory. New technologies move on from regulatory and testing procedures.

The development of a new technology and the adoption of a new ICT standard always takes time, as new regulatory requirements need to be established and the testing process needs to be organized.

To solve this problem, a process approach can be applied, as described in ISO 9001.

The PDCA cycle model is shown in Figure 7.

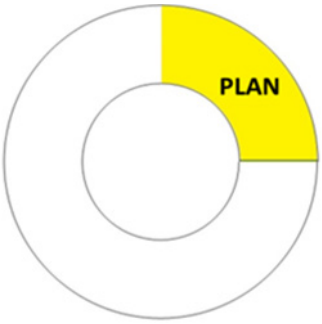
Figure 7: The PDCA cycle

Step 1 – Plan

As a first step, it is necessary to identify what new ICT standards will be implemented in the near future. Based on the results of this analysis, a report can be produced with a list of the documents needed to update the current regulatory framework, set new requirements and

develop test methods in the context of mandatory conformity assessment and compatibility testing of new equipment.

Figure 8: Plan stage of the PDCA cycle



Description of the first stage

A set of documents should be developed at the planning stage.

The documents must describe:

1. The procedure for importing the equipment into the country.
2. The specifications of the equipment needed to ensure human, animal and environmental safety.
3. The equipment needed to ensure the integrity, sustainability and security of the communication network.
4. The licences required for new ICTs (if required).
5. The procedure for bringing commercial equipment into service.
6. The testing methods for the new ICTs in the context of mandatory conformity assessment and compatibility testing of new equipment with existing equipment in the communication network.
7. The testing laboratory equipment specifications.
8. The work needed for the accreditation/validation of laboratories in order to start testing and using new methods.
9. The level of training and certification required of the staff responsible for developing and testing the new ICTs.
10. The elaboration/addition of control and monitoring measures, while ensuring compliance with established requirements.

All of these measures require time and material resources. These processes can take from one to two years. To avoid slowing the development of ICTs during this period, the review mechanism should be used.

The communication authority gives permission to a local company, which verifies that the equipment complies with the requirements by analysing the manufacturer's documents. Following a successful examination, the equipment is imported, installed and commissioned. This will remove obstacles to the deployment of pilot areas and minimize the time needed for the equipment to be commercially deployed.

Step 2 – Do

In the second stage, the work is carried out in accordance with the regulatory documents prepared, which cover the import, testing, installation and maintenance of the new ICTs. Follow-up and surveillance activities are planned to ensure compliance with the established requirements. Personnel are trained and certified in accordance with the elaborated curricula.

Figure 9: Do stage of the PDCA cycle

Description of the second stage

During the action stage, the procedures which were planned and developed in the previous step need to be carried out. This involves:

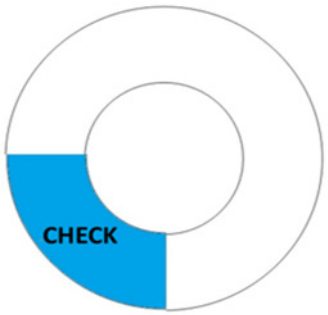
1. Certifying that the equipment complies with human, animal and environmental safety requirements.
2. Certifying that the equipment complies with the requirements for ensuring the integrity, sustainability and security of the communication network.
3. Ensuring that the new ICT equipment is imported in accordance with the relevant new import requirements.
4. Verifying the availability of the licences needed to use the new ICTs (if required).
5. Ensuring that the equipment is made commercially available in accordance with defined needs.
6. Ensuring that the testing laboratories carry out the new methods.
7. Training and certifying the staff involved in the development and testing of the new ICTs.
8. Planning and implementing control and oversight measures to ensure compliance with established requirements.

All activities and statistics related to the ICTs, including feedback from end users, are collected. During the second stage, the use of mandatory equipment and project review mechanisms is also permitted when parameters do not pose critical risks to human, animal or environmental safety.

Step 3 – Check

Once the statistics on the use of the new ICTs and the feedback from its end users have been analysed, a plan to change the current regulatory framework can be developed. Changes are introduced and the new ICTs are imported, tested, installed and operated in accordance with these changes. Monitoring and control activities are planned to ensure compliance with the adjusted requirements. Staff certification and training programmes are changed, if necessary.

Figure 10: Check stage of the PDCA cycle



Description of the third stage

In the corrective action stage, statistics and end-user feedback are analysed. Based on this analysis, changes to the following existing processes are planned and implemented:

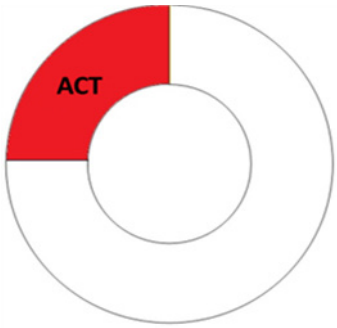
1. The compulsory certification of the equipment for compliance with human, animal and environmental safety requirements.
2. The mandatory certification of the equipment for compliance with requirements for ensuring the integrity, sustainability and security of the communication network.
3. The procedure for importing the new ICT equipment.
4. The training and certification of the staff responsible for developing and testing the new ICTs.
5. Follow-up and control measures for ensuring compliance with established requirements.

Based on the results of the corrective actions, reports are drawn up and statistical data is gathered.

Step 4 – Act

The impact of the corrective measures developed during the third stage is discussed and the future uses of the relevant ICTs are identified.

Figure 11: Act stage of the PDCA cycle



The cycle continues until the decision is made to stop using the ICTs and to dismantle the equipment. It then becomes necessary to develop requirements for the safe dismantling and removal of the equipment, and retrain the personnel who operated it.

Description of the fourth stage

In the act or decision-making stage, reports and statistics from the previous step are analysed.

Based on this analysis, changes to the following existing processes are planned and implemented:

1. The training and certification of the staff responsible for developing and testing the new ICTs.
2. Follow-up and control measures for ensuring compliance with established requirements.

Following a complete analysis of data from the entire process, the decision on whether to stop using the ICTs can be made.

6.2 C&I for 5G

6.2.1 Accreditation of laboratories and certification bodies for the use of 5G technologies

The scheduled assessments of laboratories and certification bodies (working with 5G-related technologies) must be undertaken by the ABs, taking into account the prevailing national legal and regulatory requirements. The government agency entrusted with the activity of enforcing the requirements / regulations must work closely with the AB of the economy, and the laboratories and certification bodies. This will make it easier to control and monitor the quality and interoperability aspects of 5G products. Administrations may consider benefitting from best practices and the harmonization of 5G technology. The transitional period needed to acquire the necessary new equipment and the training of specialists must be taken into account. During this period, it is advisable to use a mandatory review mechanism. It is important to benefit from the good practices and experiences of other countries.

One of the peculiarities of 5G technologies is the large number of IoT objects. Remote testing mechanisms should be established for these facilities. Unlike human users, they cannot report potential issues themselves.

Considering that the testing equipment for communication facilities and services using 5G technologies is expensive and requires the intervention of highly qualified specialists, it is advisable to set up regional centres where the necessary resources can be concentrated.

The mandatory review mechanism is promising and economically appropriate.

6.2.2 Implementation of remote testing mechanisms based on digital metrology

The quality information framework (QIF) standards are developed by the Digital Metrology Standards Consortium (DMSC™, Inc.).

QIF 3.0 was adopted as an ANSI standard in 2018 and then submitted to ISO by a technical committee in early 2019.

Based on the QIF methodology, ANSI and ISO have developed and adopted the ISO 23952:2020 standard.[37]

For the implementation of this standard, a Dimensional Measurement Interface Standard (DMIS), is provided and which provides bidirectional transmission of control data between computer systems and control equipment. It can be used as the basis for a common control system programming language. DMIS provides a programming language syntax for transferring control programs to measurement equipment and for feeding measurement and processing data back to the analysis, collection or archiving system. DMIS defines a neutral format for data exchange and is designed for human monitoring.

All these mechanisms, in turn, require communication channels calibrated for use in remote sites. For example, digital metrology is part of ICTs.

The technological basis for introducing digital metrology mechanisms is the creation of a framework for measuring sounders. Probes are installed at domain boundaries and provide a complete analysis of the transit traffic, including the origin (the actual address of the device that formed the packet), as well as all other parameters (when interacting with measurement devices to generate and analyse reference traffic).

Without digital metrology, ensuring digital sovereignty is impossible, as the origin data of the packages will not have a legally significant status, and it will not be possible to apply the current norms of international law.

6.3 Software modifications to ICT devices after certification and their impact on existing C&I frameworks

Software modifications to ICT devices after certification can have significant implications for existing C&I frameworks. These frameworks are designed to ensure that devices meet specific standards for safety, security, interoperability and performance. Here are some key points to consider regarding the impact of software modifications:

Compliance with certification standards

- **Initial certification**: when an ICT device is certified, it is assessed against specific standards and regulations. Any software modification post-certification could potentially alter the device's compliance with these standards.
- **Recertification**: depending on the nature of the modification, the device may need to undergo recertification to ensure it still meets the required standards. This can be a costly and time-consuming process.

The International Telecommunication Academy proposed a new ITU-T Recommendation project aimed at improving the compliance testing of ICT equipment with ITU standards. This proposal builds on ITU-T Recommendation Q.4068, which describes the testing process, but faces practical application challenges. The objective is to develop a new recommendation to clarify and standardize certification mechanisms.[38]

---

[37] ISO 23952:2020. Automation systems and integration – Quality information framework (QIF) – An integrated model for manufacturing quality information.

[38] ITU-D SG2 Document 2/79 from the International Telecommunication Academy.

Key points

1. Current organization of the testing system

- The testing system is based on ITU-T Recommendation Q.4068, which defines open API interfaces for the interoperable federation of testbeds.
- Technological advancements, particularly in IoT, make testing more complex and require the interconnection of testbeds to simulate real-world conditions.
- Open APIs enable the management of: the interconnection and interoperability of testbeds in a federation; the advertisement, allocation, and provisioning of resources; and user roles (experimenters).

2. Use case: experimentation in a testbed federation

- A concrete example is the experimentation of a WSN composed of IoT devices.
- Testbeds enable the performance testing of IoT devices in various environments by measuring parameters such as reliability, latency, and radio spectrum usage.
- Requirements include the relevance, reproducibility, repeatability and automation of the experiment.
- Testbed federations, such as Fed4FIRE+, provide the necessary tools to meet these requirements.

3. Use case: certification system

- The current system has shortcomings, particularly conflicts of interest when the testing laboratories are owned by the operating company.
- Test results hold an informative rather than legal status, limiting their use in case of disputes.
- The proposal advocates for the involvement of accredited, independent, and third-party certification bodies to ensure:
  - Transparent funding (via the certification authority);
  - The elimination of conflicts of interest;
  - The legal validity of test results.

4. Proposals and solutions

New Recommendation: develop an ITU-T Recommendation to clarify certification mechanisms and standardize API interfaces for federated testbeds.

Independent certification bodies

- Work with accredited organizations to ensure the impartiality, transparency, and legal validity of tests.
- Should be accredited based on national legislation, taking into account existing international good practices.

Improved interoperability: standardize API interfaces to facilitate testbed interconnection and enable reproducible and automated experiments.

This proposed solution aims to modernize and standardize ICT equipment testing and certification processes. Building on ITU-T Recommendation Q.4068, it proposes solutions to address current challenges, including IoT testing complexity, conflicts of interest and the lack of legal validity in test results. The adoption of a new recommendation and the involvement of

independent certification bodies would enhance the reliability, transparency and interoperability of compliance testing.[39]

Security implications

- **Vulnerabilities**: software updates or modifications can introduce new vulnerabilities or expose existing ones, potentially compromising the security of the device.
- **Patch management**: regular updates and patches are essential to address security vulnerabilities. However, these updates must be carefully managed to ensure they do not inadvertently introduce new risks or non-compliance issues.

Interoperability

- **Compatibility**: software changes can affect the device's ability to interoperate with other devices and systems. This is particularly critical in environments where multiple devices from different manufacturers need to work together seamlessly.
- **Standards adherence**: modifications must adhere to industry standards to maintain interoperability. Deviations from these standards can lead to compatibility issues and disrupt existing C&I frameworks.

Performance and reliability

- **Functionality**: software modifications can impact the performance and reliability of the device. Changes that affect the device's functionality can lead to failures or reduced performance, which may not align with the original certification criteria.
- **Testing and validation**: most-modification testing is crucial to ensure that the device continues to perform as expected and meet the necessary performance benchmarks.

Good practices for managing software modifications

- **Change management**: implement a robust change management process to evaluate, test and document software modifications.
- **Continuous monitoring**: establish continuous monitoring mechanisms to promptly detect and address any issues arising from software changes.
- **Stakeholder engagement**: engage with stakeholders to understand the impact of software modifications and ensure alignment with C&I frameworks.

In summary, post-certification software modifications to ICT devices can have far-reaching implications for existing C&I frameworks. It is crucial to manage these changes carefully to maintain compliance, security, interoperability and performance, while also adapting C&I frameworks to accommodate the dynamic nature of software updates.

6.4 Effective harmonization of procedures and technical collaboration

Technical collaboration and the effective harmonization of procedures are critical for ensuring seamless operations, fostering innovation and achieving shared goals in any organization or partnership. Below are key strategies to achieve this:

[39] *Ibid.*

Establish clear objectives and standards

- **Define goals:** clearly articulate the purpose of harmonization and collaboration, ensuring alignment with organizational or project objectives.
- **Standardize procedures:** develop standardized protocols, workflows and documentation to ensure consistency across teams or partners.
- **Adopt good practices:** leverage industry standards and good practices to create a common framework for collaboration.

Foster open communication

- **Regular meetings:** schedule regular check-ins, updates, and feedback sessions to maintain transparency and address issues promptly.
- **Unified platforms:** use collaborative tools (e.g. Slack, Microsoft Teams or project management software) to centralize communication and information-sharing.
- **Cross-functional teams:** encourage collaboration between departments or partners to break down silos and promote knowledge exchange.

Leverage technology

- **Integrated systems:** implement interoperable tools and platforms to streamline data-sharing and workflow integration.
- **Automation:** use automation to reduce manual errors and improve efficiency in repetitive tasks.
- **Data analytics:** utilize data-driven insights to identify bottlenecks, optimize processes and measure the impact of harmonization efforts.

Build a collaborative culture

- **Shared vision:** ensure all stakeholders understand and are committed to the shared vision and goals.
- **Trust and respect:** foster an environment of trust, respect and inclusivity to encourage open dialogue and cooperation.
- **Recognition and rewards:** acknowledge and reward collaborative efforts to motivate teams and reinforce positive behaviour.

Provide training and support

- **Skill development:** offer training programmes to ensure all team members are proficient in the tools, technologies and procedures being used.
- **Change management:** support teams through transitions by providing resources, guidance and addressing concerns.
- **Mentorship:** pair experienced team members with newcomers to facilitate knowledge transfer and skill-building.

Monitor and evaluate progress

- **KPIs and metrics:** establish key performance indicators (KPIs) to track the success of harmonization and collaboration efforts.
- **Feedback loops:** continuously gather feedback from stakeholders to identify areas for improvement.

- **Adaptability:** be prepared to adjust procedures and strategies based on evolving needs and challenges.

Ensure governance and accountability

- **Clear roles and responsibilities:** define roles and responsibilities to avoid the duplication of efforts and ensure accountability.
- **Compliance:** ensure all procedures and collaborations adhere to regulatory requirements and organizational policies.
- **Conflict resolution:** establish mechanisms to address disputes or disagreements constructively**.**

Promote innovation and continuous improvement

- **Encourage experimentation:** create a safe space for teams to experiment with new ideas and approaches.
- **Iterative processes:** regularly review and refine procedures to incorporate lessons learned and emerging trends.
- **Knowledge-sharing:** document and share successes and failures to build a culture of continuous learning.

By implementing these strategies, organizations can achieve effective harmonization of procedures and technical collaboration, leading to improved efficiency, innovation, and overall success.

6.5 How to prioritize device/type-approval models while balancing user confidence with applicable regulatory actions

In order to strike the right balance between user trust (e.g. through type approval) and compliance with regulatory measures, one must:

- Work with qualified staff to ensure the quality and effectiveness of type-approval testing
- Ensure independence in type-approval testing
- Ensure the neutral marking of test samples
- Carry out comparative tests in different laboratories

All processes in the type-approval procedure must be established by the local or regional administration.

This administration must establish and maintain a system of accreditation and verification of the activities of companies which carry out type-approval testing.

6.6 C&I challenges and opportunities during the COVID-19 pandemic

COVID-19 showed how, in a pandemic, C&I can provide:

- Warning systems;
- Outdoor access control systems;
- Indoor access control systems;
- Off-site tracking systems;

- Systems for collecting, storing and analysing information on the parameters of the pandemic;
- Systems for collecting, storing and analysing patient care information;
- Systems for collecting, storing and analysing information on the work of medical personnel;
- Systems for collecting, storing and analysing medical equipment;
- Systems for collecting, storing and analysing infection-prevention/vaccination information;
- Logistics systems for transporting and hospitalizing patients;
- Media management systems;
- Systems for international/interregional interaction.

6.7 How can new technologies contribute to improving the international C&I framework and the trade and use of ICT devices?

The following are some of the ways new technologies can help improve the international C&I framework and the trade and use of ICT devices:

- Establishing international and interregional electronic registers of permitted equipment.
- Establishing electronic document registration systems.
- Remote testing/measuring via the implementation of digital metrology mechanisms.
- Implementing common electronic registers for border and customs services.
- Harmonizing international legislation on the protection of personal data and personal information.
- Creating international/interregional information systems.
- Ensuring information security and protection of citizens, companies, State bodies.
- Maintaining unified international / interregional registers of counterfeit products.
- Implementing remote medicine mechanisms, helping people in any country.
- Implementing international/interregional disaster and emergency warning systems.

Annexes

Annex 1: Conformance and interoperability frameworks: data by country

Understanding how countries organize themselves to ensure proper C&I levels for ICT networks and device deployment can help C&I operators establish efficient collaboration mechanisms. This is evident in existing effective technical collaboration agreements, such as those in Europe and the Asia-Pacific region.

Data indicates that most countries have established C&I frameworks to ensure trust in the safe and interoperable use of ICT devices by networks and citizens. However, the procedures and the strictness of the requirements (e.g. recognition of certification, use of proxies, self-declaration and local testing) can vary significantly.

Under Pillars 3 (Capacity building) and 4 (Assistance in the establishment of test centres and C&I programmes in developing countries) of the ITU C&I programme, data was collected from 116 countries between 2022 and 2025. The research focused on key C&I infrastructure variables, namely:

1. C&I frameworks
2. ICT standards and technical requirements
3. Conformance assessment and bodies
4. Testing laboratories
5. Quality and metrology

Key findings (2022-2025)

1. C&I frameworks:
   - **85 per cent of countries** have established formal C&I frameworks.
   - **65 per cent** of these frameworks are aligned with international standards (e.g. ITU, GSMA, IEEE).
   - **Regional collaboration** has increased, with **40 per cent of countries** participating in MRAs.
2. ICT standards and technical requirements:
   - **70 per cent of countries** have adopted ICT standards based on ITU recommendations.
   - **50 per cent** have implemented additional national technical requirements to address local needs.
   - **Challenges**: the lack of harmonization in standards across regions remains a barrier to interoperability.
3. Conformance assessment and bodies:
   - **75 per cent of countries** have designated conformance assessment bodies.
   - **60 per cent** of these bodies are accredited by international organizations (e.g. ISO/IEC 17065).
   - **Gaps**: limited capacity in developing countries to conduct advanced testing and certification.

4. Testing laboratories:
   - **60 per cent of countries** have established accredited testing laboratories.
   - **45 per cent** of these labs are equipped to test advanced technologies (e.g. 5G, IoT).
   - **Challenges**: high costs and lack of skilled personnel hinder the expansion of testing capabilities.
5. Quality and metrology:
   - **55 per cent of countries** have integrated quality assurance and metrology into their C&I frameworks.
   - **40 per cent** have adopted digital tools for monitoring and reporting quality metrics.
   - **Opportunities**: the use of AI and blockchain for quality assurance is increasing.

Visual representation: histogram

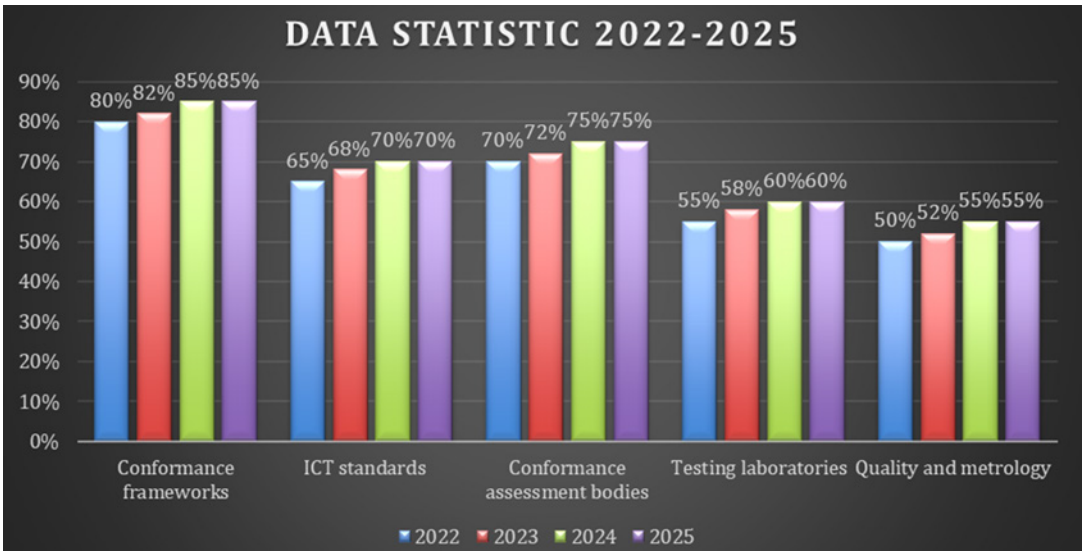
Below is a conceptual representation of the data using a bar diagram and spiral diagram to highlight trends and comparisons.

Bar diagram

- **X-axis**: C&I infrastructure variables (frameworks, standards, assessment bodies, testing labs, quality).
- **Y-axis**: Percentage of countries with established mechanisms (2022-2025).

Variable	2022	2023	2024	2025
Conformance frameworks	80%	82%	85%	85%
ICT standards	65%	68%	70%	70%
Conformance assessment bodies	70%	72%	75%	75%
Testing laboratories	55%	58%	60%	60%
Quality and metrology	50%	52%	55%	55%

Figure 12: Percentage of countries with established C&I mechanisms



- The histogram illustrates the growth trajectory of C&I frameworks and infrastructure from 2022 to 2025.
- Each loop represents a year, with the size of the loop indicating the percentage of countries adopting C&I mechanisms.
- Key variables (frameworks, standards, assessment bodies, testing labs, quality) are colour-coded for clarity.

Recommendations for 2025 and beyond

1. **Strengthen regional collaboration**: encourage more countries to join MRAs and harmonize standards.
2. **Build capacity**: invest in training programmes for conformance assessment bodies and testing laboratories.
3. **Adopt advanced technologies**: promote the use of AI, IoT and blockchain for quality assurance and interoperability testing.
4. **Provide funding and support**: provide financial and technical assistance to developing countries to establish and upgrade C&I infrastructure.
5. **Monitor and evaluate**: develop a global dashboard to track progress and share good practices.

Conclusion

The study period 2022-2025 has seen significant progress in the establishment of C&I frameworks worldwide. However, challenges such as lack of harmonization, limited testing capabilities and high costs, persist. A coordinated global effort, supported by ITU and other stakeholders, is essential to address these gaps and ensure the safe and interoperable use of ICT devices and networks.

Annex 2: Summary of the workshop on compliance and interoperability challenges for digital transformation

Friday, 2 June 2023, 0900 – 1200 hours

Workshop programme: link

This workshop was organized by the Management Team of ITU-D Study Group Question 4/2. It aimed to identify and discuss issues related to Conformance and Interoperability (C&I) of ICT equipment, with a focus on challenges facing developing countries. Discussions focused on topics related to ICT product compliance in the age of digital transformation. Participation in the workshop was open to ITU Member States, Sector Members, Associates and academia, as well as anyone wishing to contribute to the work. This included people who were also members of international, regional and national organizations.

The workshop was opened by Mr Ibrahima Sylla (Guinea), Rapporteur for Question 4/2.

SESSION 1: Future challenges and adoption in telecommunications/ICTs and digital skills enhancement for C&I

This session focused on questions related to challenges and adoption of telecommunications/ICTs and improving digital skills in developing countries for C&I, such as:

- New technologies exceeding regulations/testing procedures;
- Regulatory aspects for the adoption of openness and interoperability related to 5G;
- Software modifications of ICT devices after certification and their impacts on existing C&I frameworks;
- How new technologies can contribute to improving the international C&I framework and the trade and use of ICT devices.

Co-moderators:

- Mr Serigne Abdou Lahatt Sylla (Senegal), Vice-Rapporteur for Question 4/2
- Mr Vladimir Daigele (ITU), BDT Focal Point for Question 4/2

The first report, New conformity assessment framework for telecommunication products, was presented by Mr Leonardo Marques Campos (Brazil).

This report described how the system for confirming the conformity of communications in Brazil was arranged. Equipment was divided into groups depending on its level of influence on the communication network: either more critical or less critical. Less critical equipment shall be declared. More critical equipment was subject to certification. Particular attention was being paid to new areas - digital transformation and globalization. Voluntary cyber security certification was being offered.

The second report, Conformance and interoperability assessment in Africa: case study of Kenya, was presented by Ms Mwende Njiraini (DiploFoundation).

The report outlined how to implement compliance validation functions in a digital transformation and globalization environment, using Kenya's experience as an example.

The third report, ICT equipment certification in Russia and the Commonwealth of Independent States (CIS) region, was presented by Mr Sergei Melnik (International Telecommunication Academy)**.**

In the report, Mr Melnik noted that in the Russian Federation and the CIS region, an approach similar to the one presented in the Brazilian report was applied to confirming the conformity of communications. Algorithms for the operation of declaration and certification were given. It was noted that cyber security problems were also proposed to be solved through voluntary certification. The need to introduce digital metrology mechanisms for remote testing was especially worth noting.

SESSION 2: C&I infrastructure and applications

This session focused on**:**

- the basic infrastructure needed to obtain a quality C&I framework, from technical standards/requirements to legislative and regulatory framework revisions that would be necessary to implement appropriate C&I programmes by developing countries;
- demonstrations of C&I applications for the purposes of the mandate on national and regional experiences in C&I, good practices and possible mechanisms of collaboration for the establishment of joint programmes of C&I and technical cooperation;
- the importance of raising awareness among suppliers and users of terminal equipment in the context of improved monitoring of equipment and use of compliant equipment.

Moderator: Mr Sergei Melnik (International Telecommunication Academy), Vice-Rapporteur for Question 4/2

The first report, Combat counterfeiting through the use of RF, SAR and EMC laboratories, was presented Mr Mourad Belmrissi (Rohde & Schwarz).

The report covered the capabilities of Rohde & Schwarz equipment, advanced testing methods and the peculiarities of equipping EMC laboratories.

Mr Melnik shared his opinion on the merits of Rohde & Schwarz equipment from his own experience, especially in the field of measurement automation.

The second report, Combating counterfeit ICT devices through C&I testing and market surveillance, was presented by Mr Roland Yaw Kudozia (Ghana).

The report outlined the C&I regime in Ghana: its objective and components, technical standards and requirements, technical specifications documents, regulatory requirements, C&I testing infrastructure, market surveillance and its associated challenges, C&I awareness, the joint programme and technical cooperation with ITU, and the ITU-NCA C&I training for Africa. The speaker paid great attention to the issue of training specialists. The experience of Ghana could be very rewarding for everyone.

The third report, Conformity and interoperability of electronic communications equipment and systems: what are the contributions to digital transformation? – case of Mauritania, was presented by Mr Tidjani Oudaa (Mauritania).

Achieving these objectives necessarily required the establishment of an effective and harmonized C&I system that could assess the compliance of ICT equipment with standards

and the interoperability between competing systems, in order to build a high-quality, reliable, durable and resilient ICT infrastructure, to serve and achieve the objectives of the policy declaration for the telecommunications sector in Mauritania.

Through the analysis and evaluation of the C&I regime in Mauritania, it was clear that the country lacked the capacities and infrastructures necessary to implement conformity assessment programmes for ICT equipment and systems.

The fourth report, ICT compliance assessment in the digital transformation scenario, was presented by Mr Victor Vellano Neto (*Centro de Pesquisa e Desenvolvimento em Telecomunicações*).

The report concluded that, due to the use of several technologies in communications, hardware and software, conformity assessment was an essential part of a successful transition. Test facilities and regulatory compliance testing were therefore critical to the success of adopted solutions.

The fifth report, Overview of ITU-T SG11 activities on C&I, including C&I programme**,** was presented by Mr João Alexandre Zanon (Brazil & ITU-T Study Group 11 Working Party 4).

The report presented the results of the work. Standards for ITU-T testing had been developed. Laboratories for testing had been accredited. Mechanisms for placing and displaying test reports had been created. These mechanisms and results could be used by all countries concerned.

After the session, Mr Denis Andreev (ITU Telecommunication Standardization Bureau) spoke further about ITU-T SG11, ITU-T, how laboratories could be accredited to conduct tests and compliance with ITU-T standards, and how to view test reports in an electronic system. He invited everyone to take part in the webinar on the work of the test system.

Annex 3: Summary of the workshop on techniques designed to promote harmonization of C&I regimes

Friday, 10 May 2024, 1430 - 1730 hours

Workshop programme: see link

Background information

This workshop was designed to tackle the challenges faced by developing countries in ensuring the C&I of ICT equipment, with a special focus on countering the theft and counterfeiting of mobile devices and the regulatory aspects of IoT technologies.

The workshop was opened by Mr Ibrahima Sylla (Guinea), Rapporteur for Question 4/2.

SESSION 1: Theft of mobile devices and importance of raising awareness among equipment suppliers and users

This session explored the growing challenges of mobile device theft and the crucial importance of raising awareness among both providers and users of telecommunication/ICT equipment. With the proliferation of mobile devices in our daily lives, the risk of theft and counterfeiting of the devices had increased considerably, requiring concerted action by the entire technological ecosystem. Speakers in the session shared their knowledge and expertise on various aspects of mobile device security, including the latest technologies for tracking and combating counterfeiting, effective awareness-raising strategies, existing regulations and the need for collaboration among industry stakeholders. By focusing on preventing device theft and promoting the use of conforming equipment, the session aimed to inform participants on good practices and measures to be taken to protect data and ensure user safety.

The session was moderated by Mr Sergei Melnik (International Telecommunication Academy), Vice-Rapporteur for Question 4/2.

Theft of mobile devices and importance of raising awareness among equipment suppliers and users in Kenya

Ms Mwende Njiraini (DiploFoundation)

Ms Mwende Njiraini addressed the issue of mobile device theft in Kenya and the critical role of raising awareness among both suppliers and users. She outlined the intricacies of the regulatory framework in Kenya, which included KEBS for ISO ICT standards and the Communications Authority of Kenya for ITU recommendations. She detailed the process of type approval, the challenges faced due to the lack of a local testing laboratory, and the limited number of MRAs due to the absence of such facilities. She also discussed initiatives in Kenya to monitor and combat counterfeit ICT equipment, highlighting the KenTrade system for import verification, market surveillance efforts, and the proposed Device Management System, which had faced legal challenges but was ultimately upheld by the Supreme Court, to address counterfeit, stolen and illegal ICT devices.

Q&A session:

Questions were raised regarding the operational aspects of the Device Management System, the establishment of a laboratory for counterfeit management and the verification of

documents supplied during the type-approval process. Ms Njiraini responded by explaining the collaboration with various regulatory organizations, the proposed laboratory's role, and the current operational challenges, including trusting the authenticity of documents in the absence of a local laboratory.

Mr Papa Gueye (*École Nationale de Cybersécurité à Vocation Régionale,* Senegal)

Mr Papa Gueye provided insights into the approach of Senegal to tackling the issue of counterfeit ICT devices, highlighting the security threats they posed, including spying and data theft. He detailed legislative measures, such as competition laws, intellectual property protections, and telecommunications regulations, aimed at consumer protection. He also emphasized the need for international cooperation, public awareness campaigns and enhanced investigative capabilities to effectively combat counterfeit goods, which had significant negative impacts on national security and economic stability.

Q&A session:

An inquiry was made regarding the policy of Senegal on the protection of private data in relation to IoT devices. Mr Gueye confirmed the existence of a Data Protection Act in Senegal, which was overseen by a designated body, ensuring the safeguarding of personal data within the country.

Mobile Device Registration System

Ms Zeynep Nehir Sarıgöl (Dekob Technology)

(Ms Sarıgöl had to cancel her participation due to unexpected circumstances. Participants were invited to review the presentation available and contact her for more information.)

Overview of ITU-T activities on combating counterfeiting and stolen ICT

Mr João Alexandre Zanon (Brazil & ITU-T Study Group 11 Working Party 4)

Mr João Alexandre Zanon could not be present due to his involvement in the ITU-T SG11 Plenary occurring at the same time. Nevertheless, he provided, through a video recording, an insight into ITU-T's activities on combating counterfeit and stolen ICT devices. He brought attention to two significant resolutions, Resolutions 188 and 189 (Rev. Bucharest, 2022) of the Plenipotentiary Conference, targeting counterfeit ICT devices and mobile device theft. He discussed the work of ITU-T Study Group 11, which, since 2017, had developed various relevant recommendations, technical reports, and supplements. He emphasized the importance of a global infrastructure enabling communication between devices as well as the interoperability between various lists used in tracking problems with counterfeit and stolen devices.

Q&A session:

A question was asked about the implementation and monitoring mechanisms planned for the proposed recommendations against counterfeit ICT devices. The importance of not just presenting well-analysed propositions but also ensuring there was a system or radar in place to track the application of and adherence to these recommendations was emphasized.

As the Q&A could not be conducted in real-time due to his absence, participants were encouraged to submit their questions, which would be forwarded to him for a response.

SESSION 2: Internet of things and regulatory aspects for the adoption of the opening of C&I

This session provided an in-depth exploration of the specific regulatory challenges for the integration of IoT in the field of ICT. It brought together experts to discuss legal implications, conformance standards and interoperability strategies in the context of the increasing use of IoT in ICT infrastructures and services.

This session was moderated by Mr Sergei Melnik (International Telecommunication Academy), Vice-Rapporteur for Question 4/2.

Internet of things and regulatory aspects for the adoption of the opening of C&I

Mr Roland Yaw Kudozia (Ghana)

Mr Roland Yaw Kudozia explored the regulatory aspects and challenges pertaining to the adoption of IoT technologies. He highlighted IoT's potential for improving socio-economic conditions in developing countries, despite facing obstacles such as digital divides, security and privacy concerns, interoperability issues, and infrastructure gaps. He stressed the need for strategic planning and collaboration between governments, industry and international partners to overcome the challenges of IoT and maximize its benefits.

Q&A session:

Questions were asked about the prevalence of security flaws in IoT devices and the policies in place to protect private data. Mr Kudozia acknowledged the lack of reliable statistics on the regularity of network attacks via IoT but cited examples of devices transmitting data to unexpected servers. He confirmed that Ghana had a Data Protection Act to safeguard personal data.

A comment was also raised about the opportunity for coordination on security matters concerning new technologies and suggested that the aspects presented would be beneficial for cross-Question discussions, in particular with Question 3/2.

Conclusion

The workshop concluded with an emphasis on the multifaceted challenges of promoting C&I regimes and the pivotal role of international standards and cooperation. Participants recognized the importance of harmonized regulatory frameworks, effective MRAs, vigilant market surveillance and comprehensive consumer education to combat the theft and counterfeiting of mobile devices. Additionally, the workshop highlighted the critical need for addressing interoperability issues, particularly in the rapidly advancing IoT landscape. The consensus underscored the need for a collaborative approach by Member States, Sector members, academia, and regional and international organizations to effectively tackle the issues. The successful deployment of IoT technologies in developing countries illustrated the potential for economic development, improved access to health care and education, and enhanced resource management. However, the challenges presented by the digital divide, and the need for infrastructure development were acknowledged as significant barriers that had to be addressed through comprehensive policies, regulations and international cooperation.

Overall, the workshop served as a crucial platform for exchanging knowledge, experiences and good practices among various stakeholders in the ICT sector. The discussions reinforced the necessity of developing robust and adaptable regulatory frameworks that could keep pace

with technological advancements. The workshop's outcomes pointed towards the need for ongoing dialogue, research and collaboration to create a more harmonized and global ICT environment, which was particularly vital for the sustainable growth and development of ICT infrastructure in developing countries.

In summary, the workshop provided valuable insights into the complexities of C&I regimes and set the stage for future actions and collaborations aimed at enhancing the C&I of ICT equipment worldwide. It underlined the importance of leveraging international standards, fostering collaboration and implementing good practices to navigate the challenges and opportunities presented by emerging technologies such as IoT, ensuring their beneficial integration into society.

Annex 4: List of contributions and liaison statements received on Question 4/2

Contributions on Question 4/2

Web	Received	Source	Title
2/398	2025-04-22	BDT Focal Points for Questions 4/2 and 7/2	BDT report on the implementation of ICT Infrastructure work since the last ITU-D Study Group meeting
2/367	2025-03-31	Sri Lanka	Combating counterfeiting and theft of mobile devices
2/361 (Rev.2)	2025-05-09	Rapporteur for Question 4/2	Draft Output Report on Question 4/2
2/352	2025-03-05	Rwanda	Enhancement of institution and collaboration in combating the use of counterfeit, theft, and tampered ICT mobile devices in Rwanda
2/329	2024-10-29	Egypt	Egypt capacity building centre for African countries (EG-ATRC)
2/296	2024-10-22	China	Base station antenna OTA conformance testing practice
2/280	2024-10-28	Rapporteur for Question 4/2	Draft Output Report on ITU-D Question 4/2
2/269	2024-09-26	Sri Lanka	Proposed text for Question 4/2 Final Report, Chapter 2 "Compliance and interoperability"
2/267	2024-09-25	International Telecommunication Academy	Proposed text for Question 4/2 Final Report, Section 7.3 "Intelligent object communication paradigms"
2/266	2024-09-25	International Telecommunication Academy	Proposed text for Question 4/2 Final Report, Section 7.2 "Regulatory aspects for open and interoperable adoption related to 5G"
2/253	2024-09-19	BDT Focal Points for Questions 1/1, 2/1, 4/2, 5/1 and 7/2	BDT report on the implementation of ICT Infrastructure work since the last ITU-D Study Group meeting
2/230	2024-09-26	Rapporteur for Question 4/2	Annual progress report for Question 4/2 for November 2024 meeting
RGQ2/216	2024-04-22	Rapporteur for Question 4/2	Revised table of contents for the Final Report of Question 4/2
RGQ2/210	2024-04-18	Guinea	Draft Chapter 1 ("ICT products for the Sustainable Development Goals (SDGs)") for the Final Report of Question 4/2
RGQ2/204	2024-04-16	Vice-Rapporteur for Question 4/2	Draft Chapter 3 - Countering the proliferation of counterfeit and poor quality devices for the final report of Question 4/2

(continued)

Web	Received	Source	Title
RGQ2/203	2024-04-16	Côte d'Ivoire	Draft text for the Q4/2 Final Report, Chapter 6 ("Review of information transfer, know-how and training")
RGQ2/194	2024-04-16	BDT Focal Points for Questions 1/1, 2/1, 4/2, 5/1 and 7/2	BDT report on the implementation of ICT Infrastructure work since the last ITU-D Study Group meeting
RGQ2/186	2024-04-15	International Telecommunication Academy	Proposed text for Q4/2 Final Report, Section 7.1 ("New technologies beyond regulatory/testing procedures")
RGQ2/115	2024-02-27	Guinea	Combating counterfeiting and theft of mobile devices in Guinea
RGQ2/112	2024-02-21	Chad	Combating mobile phone theft in Chad
2/193	2023-10-16	Telecommunications Management Group, Inc.	Frameworks of conformance and interoperability to support wireless power transmission via radiofrequency beam (beam WPT)
2/189	2023-10-16	BDT Focal Points for Questions 1/1, 2/1, 4/2, 5/1 and 7/2	BDT report on the implementation of ICT Infrastructure work since the last ITU-D Study Group meeting
2/140	2023-10-03	International Telecommunication Academy	National expertise for the compliance of the ICT devices and services with the ITU standards
2/124	2023-09-14	Rapporteur for Question 4/2; Vice-Rapporteurs for Question 4/2	Annual progress report for Question 4/2 for October-November 2023 meeting
2/114	2023-09-05	Sri Lanka	Registration of legitimate mobile devices and combating counterfeiting and theft of mobile devices
2/99	2023-08-04	Liberia	Public policy challenge to combat mobile crime in Liberia
RGQ2/49	2023-04-25	BDT Focal Points for Questions 1/1, 2/1, 4/2, 5/1 and 7/2	BDT report on Future Network and Digital Infrastructure work including activities, and resources since the last ITU-D Study Group meetings
RGQ2/37	2023-04-07	Zambia	Combating the influx of counterfeit phones
RGQ2/22	2023-03-23	Madagascar	Importance of awareness-building among suppliers and users of terminal equipment in the context of improved monitoring of equipment and compliance of equipment in use
RGQ2/17	2023-03-20	Central African Republic	SDG 9 in relation to impact of counterfeit and fake telecommunications/ICTs and devices trafficked to developing countries

(continued)

Web	Received	Source	Title
2/TD/5	2022-12-06	Rapporteur for Question 4/2	Proposed workplan and table of contents for Question 4/2
2/79	2022-11-24	International Telecommunication Academy	Certification system for ICT devices and services compliance with ITU standards
2/48	2022-10-18	BDT Focal Points for Questions 1/1, 2/1, 4/2, 5/1 and 7/2	BDT report on the implementation of ICT Infrastructure work since the last ITU-D Study Group meeting
2/46	2022-10-17	Inter-Sector Coordination Group	Mapping of ITU-D Questions to ITU-T Questions and ITU-R Working Parties

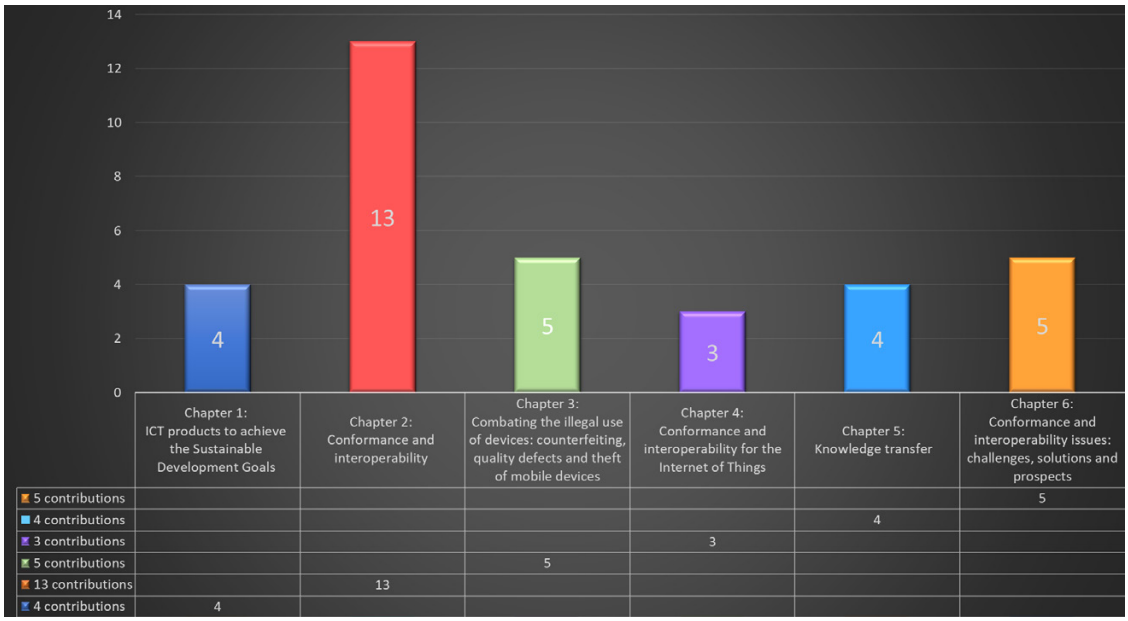
Incoming liaison statements for Question 4/2

Web	Received	Source	Title
2/357 +Ann.1	2025-03-13	International Laboratory Accreditation Cooperation	Liaison statement from the International Laboratory Accreditation Cooperation (ILAC) to ITU-D Study Group 2 Question 4/2 on the draft Final Report of Question 4/2
2/349	2025-03-20	ITU-R Working Party 5D	Liaison statement from ITU-R Working Party 5D to ITU-D Study Group 2 Question 4/2 and Working Party 1C on base station antenna OTA conformance testing
2/217 +Ann.1-2	2024-05-21	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Group 2 Question 4/2 on the progress of the work on Combating Counterfeit and Stolen Telecommunication/ICT devices/software
RGQ2/202 +Ann.1-10	2024-04-16	ITU-T Focus Group on Testbeds Federations for IMT-2020 and beyond	Liaison statement from ITU-T Focus Group on Testbeds Federations for IMT-2020 and beyond (FG-TBFxG) to ITU-D Study Groups 1 and 2 on deliverables of FG-TBFxG
2/208 +Ann.1-2	2023-10-26	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Group 2 Question 4/2 on the agreement of ITU-T Q Suppl.76 and new draft Recommendation ITU-T Q.GIR
2/207 +Ann.1	2023-10-26	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Group 2 Question 4/2 on the agreement of the Technical Report ITU-T QSTR-MCM-UC "Use Cases on the combat of Multimedia Content Misappropriation"

(continued)

Web	Received	Source	Title
2/206	2023-10-26	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Group 2 Question 4/2 on ITU Workshop "Episode 2: "Global approaches on combating counterfeiting of telecommunication/ICT devices and mobile device theft"
2/203	2023-10-24	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Group 2 Question 4/2 on ITU Tutorial on Testing Laboratories Recognition Procedure
2/93	2023-06-05	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Group 2 Question 4/2 on telecommunication/ICT equipment
RGQ2/59	2023-05-03	ITU-T Study Group 15	Liaison statement from ITU-T Study Group 15 to ITU-D Study Groups 1 and 2, Question 1/1 and Question 4/2 on contributions from developing countries
2/25 +Ann.1-4	2022-07-18	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Group 2 Question 4/2 on ITU recognition of testing laboratories
2/21 +Ann.1	2022-06-16	ITU-T Focus Group on Testbeds Federations for IMT-2020 and beyond	Liaison statement from ITU-T Focus Group on Testbeds Federations for IMT-2020 and beyond (FG-TBFxG) to ITU-D Study Groups 1 and 2 on call for use cases on testbeds federation
2/15 +Ann.1-2	2022-04-14	ITU-T Focus Group on Testbeds Federations for IMT-2020 and beyond	Liaison statement from ITU-T Focus Group on Testbed Federations for IMT-2020 and beyond (FG-TBFxG) to ITU-D Study Groups 1 and 2 on the outcomes of the first meeting of the Focus Group
2/10 +Ann.1	2021-12-21	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Groups 1 and 2 on establishment of a new ITU-T Focus Group on Testbeds Federations for IMT-2020 and beyond (FG-TBFxG) and first meeting (virtual, 4-7 April 2022)
2/8	2021-12-16	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Group 2 Question 4/2 on the progress on the combat of counterfeit and stolen ICT
2/6 +Ann.1-3	2021-12-10	ITU-T Study Group 11	Liaison statement from ITU-T Study Group 11 to ITU-D Study Group 2 Question 4/2 on ITU Testing Laboratory Recognition Procedure

Figure 13: Mapping distribution to chapters



Office of the Director
International Telecommunication Union (ITU)
Telecommunication Development Bureau (BDT)
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Office of Deputy Director and Regional Presence
Field Operations Coordination Department (DDR)
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: bdtdeputydir@itu.int
Tel.: +41 22 730 5131
Fax: +41 22 730 5484

Digital Networks and Society (DNS)
Email: bdt-dns@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

Digital Knowledge Hub Department (DKH)
Email: bdt-dkh@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

Partnerships for Digital Development Department (PDD)
Email: bdt-pdd@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

Africa

Ethiopia
International Telecommunication Union (ITU) Regional Office
Gambia Road
Leghar Ethio Telecom Bldg. 3rd floor
P.O. Box 60 005
Addis Ababa
Ethiopia

Email: itu-ro-africa@itu.int
Tel.: +251 11 551 4977
Tel.: +251 11 551 4855
Tel.: +251 11 551 8328
Fax: +251 11 551 7299

Cameroon
Union internationale des télécommunications (UIT)
Bureau de zone
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé
Cameroon

Email: itu-yaounde@itu.int
Tel.: + 237 22 22 9292
Tel.: + 237 22 22 9291
Fax: + 237 22 22 9297

Senegal
Union internationale des télécommunications (UIT)
Bureau de zone
8, Route du Méridien Président
Immeuble Rokhaya, 3e étage
Boîte postale 29471
Dakar - Yoff
Senegal

Email: itu-dakar@itu.int
Tel.: +221 33 859 7010
Tel.: +221 33 859 7021
Fax: +221 33 868 6386

Zimbabwe
International Telecommunication Union (ITU) Area Office
USAF POTRAZ Building
877 Endeavour Crescent
Mount Pleasant Business Park
Harare
Zimbabwe

Email: itu-harare@itu.int
Tel.: +263 242 369015
Tel.: +263 242 369016

Americas

Brazil
União Internacional de Telecomunicações (UIT)
Escritório Regional
SAUS Quadra 6 Ed. Luis Eduardo Magalhães,
Bloco "E", 10º andar, Ala Sul (Anatel)
CEP 70070-940 Brasilia - DF
Brazil

Email: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

Barbados
International Telecommunication Union (ITU) Area Office
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown
Barbados

Email: itubridgetown@itu.int
Tel.: +1 246 431 0343
Fax: +1 246 437 7403

Chile
Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Santiago de Chile
Chile

Email: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

Honduras
Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cía
Apartado Postal 976
Tegucigalpa
Honduras

Email: itutegucigalpa@itu.int
Tel.: +504 2235 5470
Fax: +504 2235 5471

Arab States

Egypt
International Telecommunication Union (ITU) Regional Office
Smart Village, Building B 147,
3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
Cairo
Egypt

Email: itu-ro-arabstates@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

Asia-Pacific

Thailand
International Telecommunication Union (ITU) Regional Office
4th floor NBTC Region 1 Building
101 Chaengwattana Road
Laksi,
Bangkok 10210,
Thailand

Email: itu-ro-asiapacific@itu.int
Tel.: +66 2 574 9326 – 8
+66 2 575 0055

Indonesia
International Telecommunication Union (ITU) Area Office
Gedung Sapta Pesona
13th floor
Jl. Merdeka Barat No. 17
Jakarta 10110
Indonesia

Email: bdt-ao-jakarta@itu.int
Tel.: +62 21 380 2322

India
International Telecommunication Union (ITU) Area Office and Innovation Centre
C-DOT Campus
Mandi Road
Chhatarpur, Mehrauli
New Delhi 110030
India

Email:
Area Office: itu-ao-southasia@itu.int
Innovation Centre: itu-ic-southasia@itu.int
Website: ITU Innovation Centre in New Delhi, India

CIS

Russian Federation
International Telecommunication Union (ITU) Regional Office
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation
Email: itu-ro-cis@itu.int
Tel.: +7 495 926 6070

Europe

Switzerland
International Telecommunication Union (ITU) Office for Europe
Place des Nations
CH-1211 Geneva 20
Switzerland

Email: eurregion@itu.int
Tel.: +41 22 730 5467
Fax: +41 22 730 5484

International Telecommunication Union
Telecommunication Development Bureau
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN 978-92-61-41181-7

Published in Switzerland
Geneva, 2025

Photo credits: Adobe Stock