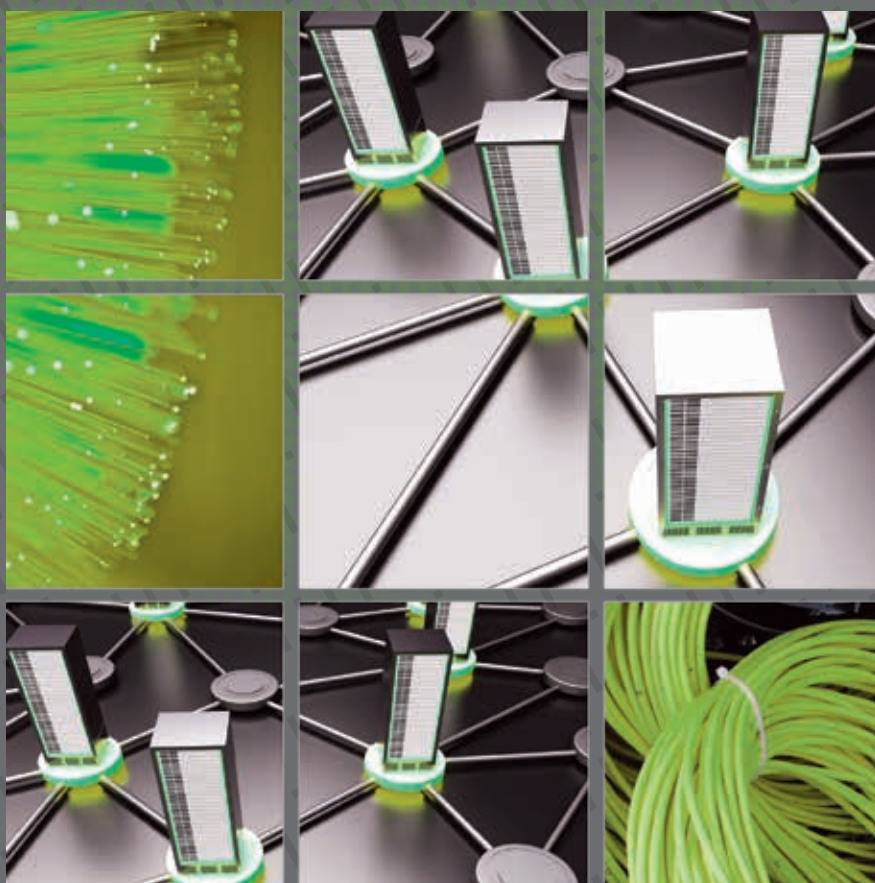


INFRASTRUCTURE

Establishing Conformity and Interoperability Regimes

Basic Guidelines



Establishing conformity and interoperability regimes: Basic guidelines

February 2014





Please consider the environment before printing this report.

© ITU 2014

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Foreword

The rapid pace of development of new ICT technologies and infrastructure has the power to affect the growth of economies and societies of both the developed and developing world. These guidelines are part of the ITU conformity and interoperability programme framework which aims to achieve an interoperable and safe global ICT communication network of networks for developing countries. The availability of high quality performing products compliant with international standards accelerates the widespread deployment of ICT infrastructure, technologies and associated services. Consequently, people are empowered with the ability to access the Information Society regardless of their location or chosen device, ultimately contributing to attaining the Millennium Development Goals.

Based on international best practices, these basic guidelines provide information for developing countries that need to plan or review their conformity and interoperability regimes for ICT products, such as procedures on different conformity assessment schemes; enabling legislation to promote the establishment of an orderly telecommunication service and equipment marketplace; methodology to calculate fees; law enforcement and surveillance; coordination with other national regulatory agencies; international standards and ICT equipment references; and compliance with the provisions of international agreements especially the World Trade Organization Agreement on Technical Barriers to Trade. Such procedures consist of general guidelines that can then be more precisely defined and tailored by the country when considering the introduction of ICT products in the market.

Many issues, challenges, questions and possibilities have been addressed in these guidelines; they offer an overview of the technological changes and administrative challenges that all ITU member countries are facing and outline possible paths towards the development of conformity and interoperability infrastructures, through the introduction of definitions, methodologies and procedures based on successful cases.

I hope that the guidance, milestones and timeframes set out in these guidelines for establishing conformity and interoperability regimes in developing countries will support and guide our Membership, and in the long run, greatly benefit their citizens.



Brahima Sanou
Director
Telecommunication Development Bureau

Contents

	<i>Page</i>
Foreword	iii
1 Definition of conformity assessment and interoperability regimes internationally accepted and standardized for the ICT sector	1
1.1 Certification	3
1.2 Supplier Declaration of Conformity (SDoC)	3
1.3 Testing laboratories	4
2 Development and review of regulatory framework and roadmap for the establishment of conformity and interoperability regimes	4
2.1 Telecommunication act provisions: Placing products in the market; institutions rights and responsibilities; identification of approved products.....	4
2.2 Methodology to calculate the fee of type approval process, including issue and/or renewal of certification.....	6
2.3 Law enforcement and surveillance; trail procedures and safeguards; post-market surveillance; sanctioning and other legal provisions and procedures.....	7
2.4 Investigation of possibilities to use the adopted conformity and interoperability regime integrated with national procedures to combat counterfeit ICT equipment in the marketplace.....	7
2.5 Coordination and harmonization of the conformity and interoperability regime with other national regulatory agencies.....	10
2.6 Mutual recognition arrangements/agreements.....	10
2.7 Harmonization of technical requirements.....	11
3 Definition and publication of ICT reference standards, interface specifications, essential requirements (electromagnetic compatibility (EMC), safety, specific absorption rate (SAR)) aimed at conformity assessment of ICT equipment	12
3.2 Consideration of World Trade Organization (WTO) rules and the Agreement on Technical Barriers to Trade	16
3.3 List of ICT equipment requiring conformity assessment	17
4 Accreditation, recognition and acceptance of laboratories and qualified professional	18
4.1 Designation/recognition of accreditation and certification bodies, and testing laboratories.....	18
4.2 Recommendations on policies and strategies for developing conformity assessment testing laboratories compliant with international standards.....	19
4.3 Recommendations on how to become accredited by international accreditation bodies (ILAC, IAF, APLAC, IECEE, etc.) in the relevant ICT scope	21
References	23

1 Definition of conformity assessment and interoperability regimes internationally accepted and standardized for the ICT sector

Service providers and operators specify standards and specifications for equipment and systems which they employ to provide services to their customers. National regulators mandate regulations, standards and specifications for equipment and systems which are deployed and used in their territories. Users of the equipment and systems along with the service providers and national regulators require evidence and proof that the equipment and systems conform to the appropriate standards and specifications and to the extent that they interoperate with each other as specified. The process used to obtain the evidence and proof is called conformity assessment – the demonstration that specified requirements relating to a product, process, system, person or body are fulfilled.

The conformity assessment committee (CASCO) of the International Organization for Standardization (ISO) has developed an extensive set of standards and guidelines that deal with all aspects of conformity assessment. These standards include:

- ISO/IEC 17000:2004 Conformity Assessment – Vocabulary and general principles
- ISO/IEC 17001:2005 Conformity Assessment – Impartiality – Principles and requirements
- ISO/IEC 17002:2004 Conformity Assessment – Confidentiality – Principles and requirements
- ISO/IEC 17003:2004 Conformity Assessment – Complaints and appeals – Principles and requirements
- ISO/IEC 17004:2005 Conformity Assessment – Disclosure of Information – Principles and requirements
- ISO/IEC 17005:2008 Conformity Assessment – Use of Management systems – Principles and requirements
- ISO/IEC 17007:2009 Conformity Assessment – Guidelines for drafting normative documents suitable for use for conformity assessment
- ISO/IEC 17011:2004 Conformity Assessment – Requirements for accreditation bodies accrediting conformity assessment bodies
- ISO/IEC 17020:2012 Conformity Assessment – Requirements for the operation of various types of bodies performing inspection
- ISO/IEC 17021:2011 Conformity Assessment – Requirements for bodies providing audit and certification of management systems
- ISO/IEC 17024:2012 Conformity Assessment – General requirements for bodies operating certification of persons
- ISO/IEC 17025:2005 Conformity Assessment – General requirements for the competence of testing and calibration laboratories
- ISO/IEC 17030:2003 Conformity Assessment – General requirements for third-party marks of conformity
- ISO/IEC 17040:2005 Conformity Assessment – General requirements for peer assessment of conformity assessment bodies and accreditation bodies
- ISO/IEC 17043:2005 Conformity Assessment – General requirements for proficiency testing
- ISO/IEC 17050-1:2007 Conformity Assessment – Supplier’s declaration of conformity – Part 1: General requirements

- ISO/IEC 17050-2:2007 Conformity Assessment – Supplier’s declaration of conformity – Part 2: Supporting document
- ISO/IEC 17065:2012 Conformity Assessment – Requirements for bodies certifying products, processes and services
- ISO/IEC 17067:2013 Conformity Assessment – Fundamentals of product certification and guidelines for product certification schemes

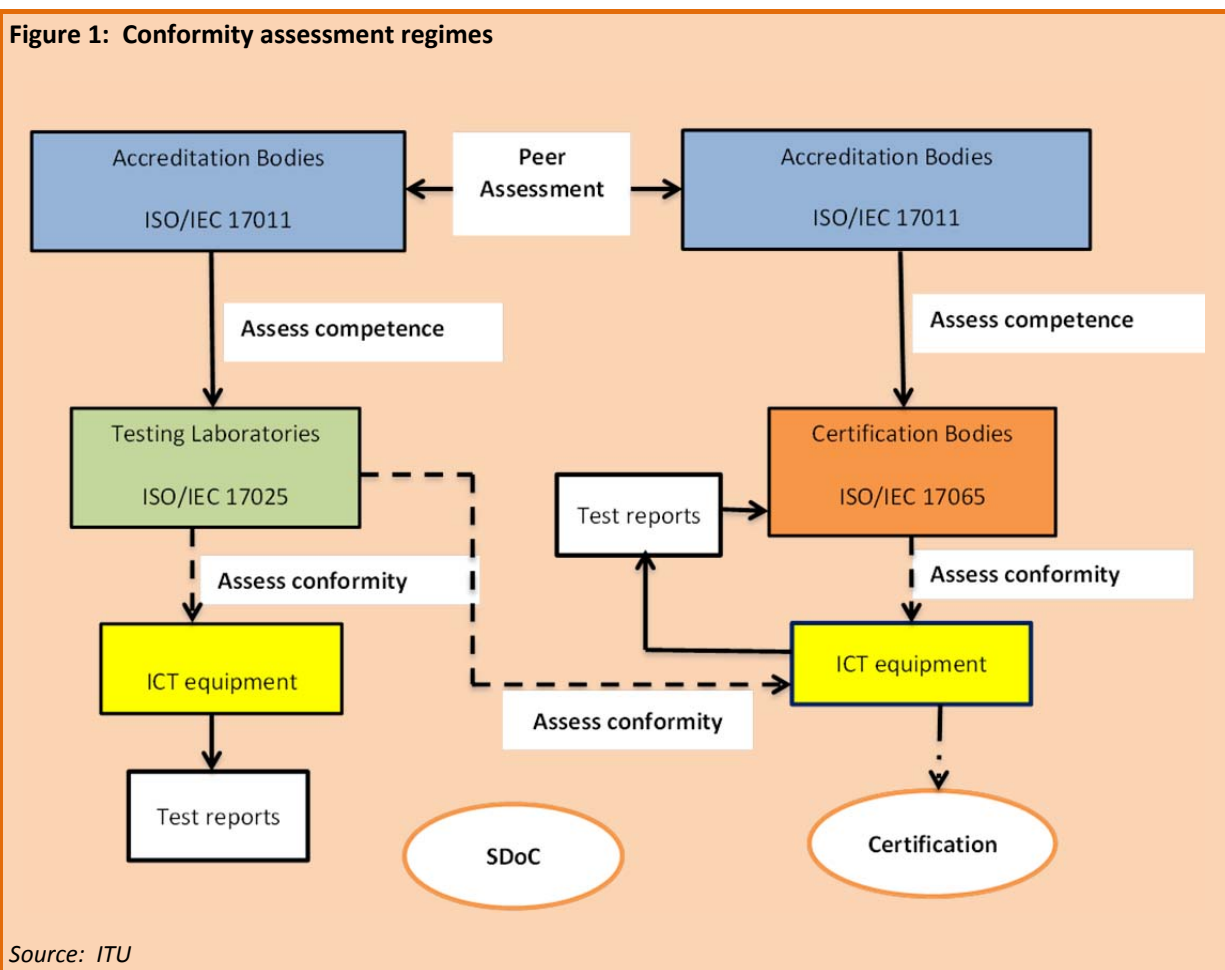
The above standards and the consideration of risk also apply in the conformity assessment regimes or schemes for the ICT sector.

When the risk and the consequences of nonconformity are low, the problems generated by nonconformity can be easily addressed and solved after they occur. In this case, the supplier declaration of conformity may be sufficient to demonstrate that the equipment conforms to the appropriate standards.

On the other hand, when the risk and consequences of nonconformity are significant, it may be necessary to obtain assurance that the equipment conforms to the requirements prior to allowing the equipment on the market or accepted by the purchasers. One method to achieve this result is called product certification.

For ICT equipment, including telecommunication equipment, the internationally accepted conformity assessment schemes are shown in Figure 1.

Figure 1: Conformity assessment regimes



1.1 Certification

Certification is a third-party attestation related to products, processes, systems or persons. Certification of equipment is the confirmation that the equipment meets the stated requisite conditions - normally indicated by the use of documentary evidence such as test reports attesting to this fact. Certification is the conformity assessment scheme employed for equipment employing new technologies and equipment which has a high degree of risk associated with non-compliance considering such aspects as safety, health or environmental impacts.

For ICT equipment, the first step towards certification is to conduct testing of the equipment by a testing laboratory which is ISO/IEC 17025 compliant. The test report produced by the testing laboratory along with the appropriate administrative information will then be sent to a third party ISO/IEC 17065 compliant certification body for certification. If the conformity assessment result is positive, the certification body will issue a certificate for the equipment. For equipment designed to meet mandatory standards, this certificate will indicate to the regulator that the equipment meets the appropriate standards. For voluntary standards, this certificate may be used by suppliers to market their equipment.

Type approval

Type approval is a special kind of certification. Type approval simply means the equipment is certified to meet certain requirement for its type, whatever that may be. Compliance to type approval requirements is often denoted by a marking on the equipment or package.

1.2 Supplier Declaration of Conformity (SDoC)

Supplier Declaration of Conformity (SDoC) is the conformity assessment scheme used for low risk and mature products. Upon meeting a set of conditions, a supplier can self-declare that the equipment conforms to the appropriate requirements (ISO/IEC 17050 and the WTO committee on conformity assessment¹). There are four different schemes of SDoC.

SDoC I (e.g. Industry Canada (Canada) conformity assessment requirement for CS-03, terminal attachment equipment)

The conditions for SDoC I are:

- testing of the equipment to be performed by an ISO/IEC 17025 compliant testing laboratory that is recognized by the regulator;
- test reports have to be kept for a prescribed period;
- supplier has to register the declaration with the regulator.

SDoC II (The FCC (USA) conformity assessment for Part 15, EMC)

The conditions for SDoC II are:

- testing of the equipment to be performed by an ISO/IEC 17025 compliant testing laboratory that is recognized by the regulator;
- test reports have to be kept for a prescribed period;
- supplier does not have to register the declaration with the regulator.

¹ WTO committee on conformity assessment:
www.wto.org/english/tratop_e/tbt_e/tbt_wrkshop_note_21march05_e.doc

SDoC III

The conditions for SDoC III are:

- testing of the equipment to be performed by a testing laboratory;
- test reports have to be kept for a prescribed period;
- supplier has to register the declaration with the regulator.

SDoC IV (eg Industry Canada (Canada) conformity assessment for ICES - 003 EMC)

The conditions for SDoC IV are:

- testing of the equipment to be performed by a testing laboratory;
- test reports have to be kept for a prescribed period.

1.3 Testing laboratories

Testing laboratories play a very important role in the operation of conformity assessment schemes including certification and Supplier Declaration of Conformity. Many regulations require that the testing laboratory has to be ISO/IEC 17025 compliant. Test reports prepared by testing laboratories are necessary information to support certification and SDoC.

2 Development and review of regulatory framework and roadmap for the establishment of conformity and interoperability regimes

2.1 Telecommunication act provisions: Placing products in the market; institutions rights and responsibilities; identification of approved products

The fundamental building block of an enforceable regime for addressing the establishment of an orderly telecommunication service and equipment marketplace is the enabling legislation. Many, if not most ITU Member States have established this legislation under various names and with varying levels of scope.

Such legislation may be found under the national Telecommunication Act, Radiocommunication Act, or created as a combined act including telecommunications, radiocommunication and possibly other elements such as calibration and fees for services aspects². Such acts are “the law of the land” and are further interpreted by regulatory requirements that deal with such practical matters as penalties for infractions, fees, obligations of parties, importation, market surveillance and so on.

For the purpose of these basic guidelines, the term telecommunications act is used to refer to the general case with a particular focus on the regime of telecommunication equipment, including radiocommunication apparatus, broadcast equipment, and electromagnetic radiation aspects.

A telecommunication act reflects the policy of the sovereign state in question and can include a clear statement of the underlying policy. This statement would cover such elements as:

- orderly development of a telecommunication system;
- reliable and affordable telecommunication services of high quality;
- highlighted role of telecommunications to enhance efficiency and competitiveness;

² Canadian Telecommunications Act: [http://en.wikipedia.org/wiki/Telecommunications_Act_\(Canada\)](http://en.wikipedia.org/wiki/Telecommunications_Act_(Canada))

- efficient and effective regulation where required;
- support for research and development and encouragement of innovation for the provision of telecommunication services;
- responsiveness to the economic and social requirements of users of telecommunication services;
- contribution to the protection of the privacy of persons.

Telecommunication legislation can also address the following key areas:

Operational matters:

- ownership and control of services and facilities;
- international telecommunication services and licenses;
- regulations pertaining to service provision.

Rates, facilities and services:

- provision of services;
- connection of facilities;
- provision of information;
- telecommunication numbering and related matters.

Telecommunication apparatus and administration:

- application to apparatus subject to regulation;
- government powers and exercise of powers;
- certification and marking;
- appeals and evidence;
- regulations including fees and mandatory requirements.

Investigation and enforcement:

- administrative and monetary penalties;
- offences;
- inspection and market surveillance;
- forfeiture;
- civil liability.

Thus in summary the provisions of a typically well formulated telecommunication act addresses all foreseen issues arising from placing telecommunication products in the marketplace. These include the rights and responsibilities of institutions as regards enforcement and related matters, the necessity of identification of approved products and record keeping, and operational matters including ownership and civil liability.

2.2 Methodology to calculate the fee of type approval process, including issue and/or renewal of certification

Schedule of Fees

Fees are based on the principle of recovery of costs. The number and type of fees vary from country to country but in general there are four types of fees applicable in the type approval process. The two most basic fees are those for assessment of conformity to the regulatory requirements, and the fee for the technical expertise required to perform the assessment. Beyond that there may be a fee for registration of the product and related data and a further fee for listing on a publicly available database of products approved for deployment in the marketplace in question.

In some jurisdictions radiocommunication licensing fees for service providers are deemed to include a fee for purposes of registering hands-free equipment and in such cases there is no separate registration fee for such apparatus.

Assessment and reassessment fee

The assessment and reassessment fee relates to administrative costs involved in reviewing certification applications to ensure that the equipment complies with the appropriate technical requirements, specifications or standards. This fee is assessed per product model regardless of the number of standards being assessed. The fee includes a charge for the administration of the application, the technical examination, and the review of the brief and the issuance or renewal of a technical acceptance certificate.

Technical expertise fee

Technical expertise may be provided by the type approval authority for services such as assistance in evaluating the technical competence of conformity assessment bodies, performing reassessment, as well as reviewing applications for multiple listings, family approval or transfer of a technical acceptance certificate (TAC) . This fee would also include equipment set-up time, testing time, report preparation, examination and approval of the report by the laboratory supervisor. This fee is calculated at the established rate per person-hour or part thereof of the type approval authority in the relevant jurisdiction. Upon request, a type approval authority can usually provide an estimate of the cost for testing services or technical support to its clients. The type approval authority may request full payment of the estimated cost before service is provided in order to be assured of cost recovery. Progress payments would normally be required for situations where longer than normal test times are needed. In cases where travel is required, travel expenses are also be factored into the estimated cost.

Listing fees

The listing fee is for the administration required to record the equipment in the relevant list of approved apparatus. This fee applies to each product model listed.

Registration fees

As part of the conformity assessment process, equipment may also require to be registered with the type approval authority. In this case a registration fee is assessed to cover the development and maintenance cost of the approval programme and the administration required in recording the equipment on the list of approved products. This fee may apply to each product model listed or to a family of products that are electrically identical.

Payment of fees

In the general case fees are payable before services are rendered. For example, in most cases, the fee is payable at the time of making the application for assessment, reassessment, listing and/or registration.

2.3 Law enforcement and surveillance; trail procedures and safeguards; post-market surveillance; sanctioning and other legal provisions and procedures

Market surveillance

The objective of market surveillance of deployed telecommunication equipment is to ensure that products placed on the market do not cause electromagnetic interference, harm the public telecommunication network, and endanger health, safety or any other aspect of protection of public interests.

In practice, market surveillance includes any necessary action (e.g. prohibitions, withdrawals, recalls) to stop the circulation of products that do not comply with all the requirements set out in the relevant legislation and regulations, to bring the products into compliance and to apply sanctions.

Market surveillance is vital to the smooth functioning of the telecommunication marketplace. It is essential in protecting consumers and workers against risks presented by non-compliant products. In addition, market surveillance helps to protect responsible businesses from unfair competition by unscrupulous economic operators who ignore the rules or cut corners. Many regulatory bodies worldwide have specific legal requirements for the organization of market surveillance.

Regulations characteristically set out clear obligations for market surveillance authorities, stipulating that they must have the necessary powers, resources and knowledge to properly perform their functions. The regulation requires procedures to be put in place for following up complaints, monitoring accidents, verifying that corrective action has been taken and gathering scientific and technical knowledge concerning safety issues. In addition, ITU Member States must establish, implement and periodically update national market surveillance programmes and review and assess the functioning of their surveillance activities periodically e.g. every few years.

Typical market surveillance activities may include: organizing random and targeted spot checks; obtaining all necessary documentation from manufacturers to evaluate product conformity; when justified, entering manufacturer premises and taking samples for testing; and in extreme cases destroying products or requiring complete product recall of the non-compliant models. If authorities find products presenting a risk, they must alert other potential users of those products, including telecommunication service providers, to reduce the risk of further injury or harm to either persons or the public telecommunication network. Products which present a serious risk, requiring rapid reaction, must be recalled from the market or measures must be taken in order to ensure that they do not reach the market.

Information exchange and effective cross-border co-operation between market surveillance authorities in different ITU Member States is very helpful in ensuring efficient, comprehensive and consistent market surveillance in the region. Mutual recognition arrangements/agreements on conformity assessment of telecommunication equipment among like-minded regulatory authorities can facilitate such trusted cooperation, based on robust credentials of the participants.

2.4 Investigation of possibilities to use the adopted conformity and interoperability regime integrated with national procedures to combat counterfeit ICT equipment in the marketplace.

The fast development of the information society has led to the arrival of new problems associated with the counterfeit of ICT equipment. One of the most important problems is in regard to protecting intellectual property items, including software, and ICT products including mobile telecommunication products which have attracted more than their share of counterfeit attacks. At present in many countries, including countries with developed economies, the legislation has proved to be unprepared to resolve such issues although this is changing with a number of countries introducing targeted legislation dealing explicitly with fraud and counterfeit. This is one of a number of key problems associated with the development of an information society. Legislation must be backed up with market surveillance and enforcement with stiff penalties for infractions in order to be effective.

Combatting counterfeiting

ITU-T Study Group 11 is presently developing a comprehensive report on counterfeit equipment, available on the TIES website presently in draft form as Temporary Document 0256 (GEN11). This draft report expands on an excellent technical report finalised by an external ITU expert. The following section is adapted from the SG 11 draft report³.

One very basic tool for combatting counterfeiting is by marking products so that they can be authenticated. Labels and embossing that are difficult to forge can be attached to products and serial numbers assigned that can be used to authenticate that the item is genuine. This approach has been used in the telecommunication equipment industry for many years. Nevertheless mobile phones are especially targeted with some 250 million counterfeits sold that constitute an estimated 15-20 per cent of the global market in terms of units sold annually. This shows that such robust marking is by no means fool proof and that the mobile telecommunication customer equipment market in particular is rife with counterfeit equipment. Even government sanctioned regulatory markings with stiff penalties for infractions have failed to dissuade counterfeiters.

Strict control of supply chains, and possibly of complete product lifecycles, is required with testing and certification as necessary to ensure that quality standards are met. In addition, customs officials need to be given the tools to identify counterfeit products and market surveillance and enforcement measures may be employed. In addition importers with a track record of ignoring import controls can be identified and put on a special list. When shipments of ICT equipment are being imported by rogue importers regulatory authorities can be notified so that a decision can be made to carry out inspections and enforcement should this be warranted.

The legal instruments to combat counterfeiting are largely in place but enforcement is still weak. The 2008 OECD report on the economic impact of counterfeiting⁴ concluded that the “magnitude and effects of counterfeiting and piracy are of such significance that they compel strong and sustained action from governments, business and consumers. More effective enforcement is critical in this regard, as is the need to build public support to combat the counterfeiting and piracy. Increased co-operation between governments, and with industry, would be beneficial, as would better data collection.”

Some countries, such as Columbia for example have taken direct action to combat counterfeiting. In 2011 the Ministry of Information and Communication Technologies of Colombia issued Decree 1630 for the purpose of establishing mechanisms aimed at controlling the marketing and sale of both new and used terminal devices and creating two types of centralized databases, one that has a registry of the International Mobile Equipment Identity (IMEI). The draft report highlights the concrete actions of some 12 countries and two major regional bodies in combatting counterfeit products⁵.

International Mobile Equipment Identity (IMEI)

As already noted mobile phones have been a particularly attractive target for counterfeiters and, in response, the Mobile Manufacturers Forum (MMF) has created a website giving information for consumers on how to spot counterfeit phones and batteries - spotafakephone.com. They advise that one should get to know the appearance, capabilities, availability and price of the genuine articles and also check the IMEI (International Mobile Equipment Identity) number. The IMEI is a unique identifier for each

³ ITU SG 11 TD GEN 0256 Draft Technical Report on Counterfeit Equipment: www.itu.int/md/T13-SG11-131107-TD-GEN-0256/en

⁴ OECD ICCT Product Classification Report: www.oecd.org/sti/ieconomy/2771160.pdf

⁵ ITU SG 11 TD GEN 0256 Draft Technical Report on Counterfeit Equipment: www.itu.int/md/T13-SG11-131107-TD-GEN-0256/en

mobile phone and counterfeits often do not have an IMEI or have a fake number. A tool to check the validity of an IMEI is provided by International Numbering Plans⁶.

Today, there are a number of systems based on IMEI registration, which are operated or planned by individual administrations and regulatory authorities to identify genuine and legally imported mobile terminals. Different regional initiatives and approaches have been already launched to implement national, regional and international actions and measures for information exchange on mobile terminal devices of illegal origin. To assist the regulatory authorities in protecting consumers, operators and governments from the negative effects of counterfeit mobile devices, the regional regulatory associations recommended that ITU will conduct studies and provide guidelines and recommendations.

International standards development bodies are also active in the fight to combat counterfeiting. Among these, International Committee ISO/IEC 15459⁷ defines unique identifiers for supply chain tracking that can be represented in Automatic Identification and Data Capture (AIDC) media such as barcodes and RFID.

ISO Technical Committee 246 is chartered to produce standard anti-counterfeiting tools. This committee is developing a standard on the performance criteria for authentication solutions for combating the production of counterfeit goods⁸.

The ITU-T is working on systems for accessing multimedia information triggered by the tag-based identification of things. As part of this work a description of the various Identification (ID) schemes that could be used for such identification of, for example ICT products, is being produced. ITU-T Recommendation X.668⁹ provides an important tool for specifying the information and justification to be provided when requesting an Object Identifier (OID) for such identification schemes, and the procedures for the operation of a registration authority.

ITU engagement

Resolution 177 of the 2010 Plenipotentiary Conference of the ITU *“invites Member States and Sector Members to bear in mind the legal and regulatory frameworks of other countries concerning equipment that negatively affects the quality of their telecommunication infrastructure, in particular recognizing the concerns of developing countries with respect to counterfeit equipment”*¹⁰.

ITU Member States have indicated that counterfeit equipment is having a measureable impact on conformity and interoperability problems. According to the ITU Guidelines for developing countries on establishing conformity assessment test labs in different regions¹¹, it is noted that:

... suspicion of dumping of sub-standard products in the marketplace which have failed testing in other countries is a further cause of concern as is the importation and deployment of counterfeit products. A key component of the answer to such concerns is to have a robust

⁶ International Numbering Plans: www.numberingplans.com/?page=analysis&sub=imeinr

⁷ ISO 6346 Freight containers -- Coding, identification and marking

⁸ Unique ID Coding: www.uidcenter.org/learning-about-ucode

⁹ ITU-T Recommendation X.668: Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: Registration of object identifier arcs for applications and services using tag-based identification

¹⁰ Plenipotentiary Conference of the International Telecommunication Union (Guadalajara, 2010) Resolution 177: www.itu.int/ITU-D/tech/NGN/ConformanceInterop/PP10_Resolution177.pdf

¹¹ Guidelines for developing countries on establishing conformity assessment test labs in different regions: www.itu.int/ITU-D/tech/ConformanceInteropability/ConformanceInterop/Guidelines/Test_lab_guidelines_EV8.pdf
Published by the ITU Telecommunication Development Bureau in May 2012.

type approval regime and test laboratories working from a set of technical standards, a testing regime and testing capability to approve and monitor communications technologies which are being deployed on the marketplace, backed up by surveillance, audit and enforcement. If there are no established technical requirements, type approval regime and test laboratories available to a country or region then the marketplace is left largely unprotected.

2.5 Coordination and harmonization of the conformity and interoperability regime with other national regulatory agencies

Design and implementation of a new telecommunication regulatory regime, together with the necessary up-front policy and legislative work, is a daunting task. A fully developed regulatory system requires a trusted and recognized accreditation system, testing laboratories, certification bodies, market surveillance, and audit and enforcement capabilities to determine compliance and assess penalties for non-compliance. The absence of any one of these components may result in the regulations having little positive impact on compliance in the marketplace.

These challenges all have significant financial and expert resource implications. Consequently, some developing countries have adopted an interim measure in lieu of establishing their own regulatory system namely by recognizing regulatory and certification marks of other jurisdictions. These then are used as mandatory requirements for importation and deployment of telecommunication equipment in their marketplaces. Amongst such recognized markings are those of the EU, FCC, IC and Anatel, and in some cases all four or even additional marks. The benefit of such an approach is that it can reduce the level of chaos in the marketplace with minimal investments by the regulatory or government authority, and within a short timeframe. Potential shortcomings of the approach can include the problem of remaining up to date with what technical requirements underpin the mark, deviations in local requirements from foreign marked product capabilities, and no real laboratory capability to assess compliance with adopted marks.

2.6 Mutual recognition arrangements/agreements

Another approach to the financial, expertise and resource problems mentioned above may be possible through sharing of facilities using the instrument of mutual recognition arrangements/agreements (MRAs). MRAs on conformity assessment of telecommunication equipment are already in operation in many world regions, between and among countries and between regions. In such cases MRAs based on appropriately robust credentials of the parties and agreed operational processes can permit a wide spectrum of sharing of facilities and services. For example, under an MRA a test laboratory in one country can avail itself of accreditation services from another country, provide certification and testing of products from a third country and affix marks and ship products directly to foreign MRA partner countries. The advantage of the MRA approach is that none of the partner country technical or administrative requirements need to be harmonized. The MRA simply recognizes and accepts the competence of the MRA partner to carry out its defined and agreed regulatory procedures. These may be limited to production of test result for purposes of certification, or include both testing and certification and marking.

MRA benefits¹²

A number of important benefits accrue from MRAs. MRAs on conformity assessment are intended to promote efficiency and sharing of conformity assessment resources and to streamline the flow of

¹² www.itu.int/en/ITU-D/Technology/Documents/ConformanceInteroperability/GuidelinesMRAs_E.pdf.

products amongst participating parties which may include ITU Member States, government agencies and departments, private sector organizations such as testing laboratories, certification bodies and accreditation bodies. MRAs provide for the recognition of competence of third parties to carry out national regulatory/type approval processes such as mandatory testing and certification, or testing and certification of products conforming to non-regulatory requirements. MRAs have the potential to reduce the cost of carrying out testing and/or certification due to facilitating integrated manufacturing, testing and certification for target markets, which in addition can significantly reduce time to market. In the regulatory sector they permit obtaining the required national certificates for products locally by manufacturers, help avoid rejection of consignments of products and eliminate redundant procedures. In the non-regulatory case they provide a basis for sharing of testing and certification services among parties with the establishment of trust based on agreed credentials and usually evidenced by a formal certification process.

A further benefit of MRAs is that they promote transparency in market access. For example in MRAs dealing with regulated products they constrain the parties to follow the agreement which spells out in detail the procedures for market access. This has a major impact on removal of predatory and non-transparent procedures which may favour national industries and deny national treatment to other signatory parties thereby damaging the competitive edge of those parties in that marketplace. Estimates of savings obtained through MRAs are based on the elimination of re-testing, re-shipment to destination marketplaces for certification, and removal of the need for local staff of the originating party to be present in the destination marketplace to handle the interface with testing laboratories, accreditation and certification bodies.

MRAs dealing with regulated products have most meaning when there is a regulatory system in place in the marketplaces of the signatories, specifying among other things mandatory technical requirements and procedures for products to be legally in the marketplace. Therefore an additional side benefit of such MRAs is to raise the awareness of the need for and benefits of a regulatory system which prevents harmful interference amongst deployed systems and prevents both network harm and harm to persons using or working with telecommunication products and systems. Such regulatory systems may also be said to reflect the value system of the society in which they are deployed since they specifically address safety of life and interference-free service delivery to the marketplace.

2.7 Harmonization of technical requirements

A further approach is that of harmonization of technical and/or administrative procedures. This approach may be possible between and amongst parties with very similar regulatory requirements. However in some jurisdictions, even those with very similar technical and administrative procedures, it has proved difficult to achieve success. The difficulties include coordination of deviations in technical specifications and therefore test suites, differences in regulatory philosophies, scope of regulations and so on.

So one pragmatic way forward for a region with like-minded authorities and similar problems in scarcity of resources and funding for a fully developed national telecommunication regulatory system could be to establish a forum, or use an existing one to discuss how to proceed in a cooperative way to deal with this matter. A framework MRA for example could provide the basis for such a cooperative effort. The discussion would then focus on how to establish shared accreditation, testing and certification capabilities, on what basis these would be funded, how to acquire and deploy the needed expertise, recover costs, establish fees, survey and enforce compliance in the marketplace, etc.

3 Definition and publication of ICT reference standards, interface specifications, essential requirements (electromagnetic compatibility (EMC), safety, specific absorption rate (SAR)) aimed at conformity assessment of ICT equipment

Basic international standards, standards development processes and case examples covering the essential requirements for ICT products (e.g. health and safety, EMC, protocols, interfaces)

In the context of these guidelines the pre-eminent category of ICT products under consideration is those with telecommunication capabilities. In this field, a specific large sub-category of equipment has mandatory technical specifications as part of the regulatory requirements which must be met in order to be deployed in the marketplace. These requirements (essential requirements) may be expressed in discrete categories as follows: Broadcasting equipment standards, radio equipment standards, digital television standards (DTV), electromagnetic compatibility standards, standard radio system plans (SRSP) and Terminal Equipment - Technical Specifications.

These standards are developed primarily in accordance with decisions made and ratified in the International Telecommunication Union (ITU), International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) combined with regional, national and industry standards requirements and are therefore a complex and very complete set of requirements which are vitally important to an interference free and safe environment for ICT products. A number of regional standards bodies serving specific regional policies, regulations and requirements are heavily engaged in development and promulgation of the product standards and include the European Telecommunications Standards Institute, USA Telecommunications Industry Association, and various important forums and consortia such as 3GPP.

The process to arrive at many of these equipment standards and specifications, especially in the radiocommunication equipment side stems primarily from basic work of the ITU membership at the World Radiocommunication Conferences (WRCs) where decisions are made regarding what services are to be defined in specific frequency bands. This in turn guides national and regional decisions on determining their frequency band plans for various services including broadcast and other radiocommunication services and usage. Following this, frequency band plan guides are developed for national and regional frequency allocations, known as standard radio system plans¹³.

The final step is the development of radio equipment standards which establish the frequency spectrum masks for the radiocommunication equipment taking into account band separation, filtering, signal power levels and so on. Table 1 is an extract from the conformity and interoperability assessment study¹⁴ carried out in the Southern African Development Community (SADC) region and done for the ITU regional office and headquarters by eminent telecommunication consultants from the African region. It gives concrete examples of international standards, regional standards and forum and consortia standards used in the SADC region.

¹³ Canadian Spectrum Management and Telecommunications Regulations: www.ic.gc.ca/eic/site/smt-gst.nsf/eng/home

¹⁴ ITU report on Conformity and interoperability assessment on a regional basis, Southern African Development Community (SADC) - draft final report: www.itu.int/en/ITU-D/Technology/Documents/ConformanceInteroperability/SADC%20Assessment%20Study_Final_November13.pdf

Table 1: Example of reference standards and products

Category	Product	Standard	Technical requirement
User equipment	Mobile	3GPP	Power; frequency stability, frequency in-band emission.
	Landline phone	IEC	Electrical, sound pressure, acoustic chock protection
	PABX	<ul style="list-style-type: none"> ITU-T Rec. G.711: Pulse code modulation (PCM) of voice frequencies ITU-T Rec. Q.921: ISDN user-network interface – Data link layer specification 	Protocols
	Charge and power adapter	ITU-T Rec. L.1000	Power, energy efficiency, eco-environment specifications
	Personal area communication	National Frequency Allocation	Gain, transmission power, bandwidth, frequency stability.
	Residential optical unit	ITU-T G.984	Power; frequency stability, frequency in-band emission, SAR limits.
	UTP cable	ISO/IEC 11801	Return Loss, FEXT, NEXT, bandwidth
RTTE	Mobile - Broadband base station	ETSI	Gain, transmission power, bandwidth.
	Antenna	ETSI	Radiation Diagram, Gain, VSWR.
	Broadcast transmitter	ETSI	Gain, transmission power, frequency width.
	Earth station equipment / VSAT	ETSI	Gain, transmission power, bandwidth.
Network equipment	Transmission equipment	ITU-T Rec. G.707	Protocols
	Network switches and routers.	MPLS - G.8121 Ethernet - G.8021 IPTV - H.62X	Protocols
	Cables	ISO/IEC 11801	Return Loss, FEXT, NEXT, bandwidth
	IPTV	ITU-T Rec.	See Standard
Electromagnetic compatibility	All equipment	ITU-T Rec. K.48	Radiated spurious emission, conducted spurious emission, resistibility
Safety	All equipment	ITU-T Rec. K.21	Electrical chock protection, fire protection, overcurrent protection

The section below provides another example of how these kinds of standards are structured in a particular Member State (in this case Canada)¹⁵.

¹⁵ Full details on each element can be seen at the following website and are therefore not repeated in this report: www.ic.gc.ca/eic/site/smt-gst.nsf/eng/h_sf01375.html.

Broadcasting equipment standards

- Broadcasting Equipment Technical Standards (BETS)
- Broadcasting Specifications and Standards (BTS & BS)
- Broadcasting Certificate Exempt Radio Apparatus List

Radio equipment standards

- Radio Standards Specifications (RSS)
- Category I Equipment Standards List
- Category II Equipment Standards List
- License-exempt Radio Apparatus Standards List
- Regulatory Standards Notice

Digital television standards (DTV)

- Digital Audio Compression Standard
- Digital Television Standard

Electromagnetic compatibility standards

The following series of standards are largely adopted or adapted from the CISPR (International Special Committee on Radio Interferences) standards.

- Industrial, Scientific and Medical (ISM) Radio Frequency Generators
- Vehicles, Boats and Other Devices Propelled by an Internal Combustion Engine, Electrical Means or Both New
- Spark Ignition Systems of Vehicles and Other Devices Equipped with Internal Combustion Engines
- Information Technology Equipment (ITE) - Limits and methods of measurement
- Alternating Current High Voltage Power Systems New
- Radio Frequency Lighting Devices
- AC Wire Carrier Current Devices (unintentional radiators)

Standard radio system plans (SRSP)

Standard radio system plans are an important component of an interference free regulatory system for radiocommunication. Among other purposes they state the minimum technical requirements for efficient use of the frequency band for which they are developed. While they are not generally comprehensive specifications for equipment design, they include important information that promotes efficient spectrum usage in the related apparatus. Issues such as channel spacing, coordination of adjacent blocks of spectrum, coexistence among radio systems in adjacent bands and out of band emission concerns are treated in these SRSPs.

Some examples are given below, taken from the Canadian Spectrum Management and Telecommunication website¹⁶ where publicly available information is available for a wide range of radiocommunication services.

- SRSP-300.512 - Technical Requirements for Remote Rural Broadband Systems (RRBS) Operating in the Bands 512-608 MHz and 614-698 MHz
- SRSP-302.0 - Technical Requirements for Fixed Line-of-Sight Radio Systems Operating in the Bands 2025-2110 MHz and 2200-2285 MHz
- SRSP-302.3 - Technical Requirements for Wireless Communications Service Operating in the Bands 2305-2320 MHz and 2345-2360 MHz
- SRSP-303.65 - Technical Requirements for Wireless Broadband Services (WBS) in the Band 3650-3700 MHz
- SRSP-338.6 - Technical Requirements for Fixed Radio Systems Operating in the Band 38.6-40.0 GHz
- SRSP-503 - Technical Requirements for Cellular Radiotelephone Systems Operating in the Bands 824 - 849 MHz and 869 - 894 MHz
- SRSP-508 - Technical Requirements for Digital Cordless Telephone (DCT) Systems Operating in the Band 944 to 948.5 MHz
- SRSP-513 - Technical Requirements for Advanced Wireless Services in the Bands 1710-1755 MHz and 2110-2155 MHz

Terminal equipment: Technical specifications/standards list

This is an 8-part standard which provides the technical requirements for connection of terminal equipment to public networks and for hearing aid compatibility with handsets. It contains the compliance specifications for terminal equipment, terminal systems, network protection devices, connection arrangements and hearing aid compatibility.

Specific absorption rate (SAR): Limits of human exposure to radiofrequency electromagnetic energy in the frequency range from 3 kHz to 300 GHz

The limits of human exposure to radiofrequency electromagnetic energy take into account the total RF exposure from all sources of RF energy. For example, in a given area, the combined RF energy from all cell towers and other wireless infrastructure are not to exceed the limits in specified by the national body responsible for establishing these limits. These limits are normally established by the national body responsible for the health of the public in ITU Member States (e.g. Department of Health or equivalent agency). Therefore, no adverse health effects are expected from exposure to RF emitting devices if the devices adhere to these limits. This is the case for cellular towers and cellular telephones.

As a practical example, in Canada the exposure limits have been established by scientific studies related to thermal and possible non-thermal effects of RF energy on biological systems. Safety factors have been incorporated into these limits to add an additional level of protection. A safety factor of 10 has been incorporated for exposures in controlled environments such as radio tower facilities. A safety factor of 50 has been incorporated for exposures in uncontrolled environments such as in use of cellular phones. The regulation in this matter in Canada is known as Safety Code 6¹⁷ and is the responsibility of the Department of Health.

¹⁶ www.ic.gc.ca/eic/site/smt-gst.nsf/eng/h_sf06130.html

¹⁷ Safety Code 6 and SAR: www.c4st.org/safety-code-6

Specialized measurement systems have been developed to permit determination of the SAR value of a given product or system in order to assess compliance with the Safety Code 6 or similar standard in another jurisdiction. Operation of these systems, which may include the use of special fluids to simulate brain and body fluids, robotics for automated measurements and probing, mannequins to simulate body parts and other highly technical equipment require specialized training.

3.2 Consideration of World Trade Organization (WTO) rules and the Agreement on Technical Barriers to Trade

The World Trade Organization (WTO) is the international organization whose primary purpose is to open trade for the benefit of all¹⁸. The WTO Agreement on Technical Barriers to Trade¹⁹, commonly referred to as the TBT agreement tries to ensure that regulations, standards, testing and certification procedures do not create unnecessary obstacles, while also providing members with the right to implement measures to achieve legitimate policy objectives, such as the protection of human health and safety, or the environment. It is therefore an important recommendation that unless there are overriding national considerations, technical specifications, procedures and requirements for ICT products should be based on open and transparent international standards and norms.

Technical regulations and product standards may vary from country to country but having many different regulations and standards makes life difficult for producers and exporters. Furthermore technical standards and regulations could be used as an excuse for protectionism, in effect becoming an intentional technical barrier to trade.

The principles of the TBT agreement are as follows: (1) Avoidance of unnecessary obstacles to trade; (2) Non-discrimination and national treatment; (3) Harmonization; (4) Equivalence of technical regulations; (5) Mutual recognition of conformity assessment procedures; and (6) Transparency. For example, members shall accord equal treatments for other members on technical regulations, standards and conformity assessment procedures to all products, including ICT products. The agreement also requires members to use relevant international standards or to use a part of relevant parts of them if they exist, as a basis for their technical regulations, standards and conformity assessment procedures²⁰.

The Technical Barriers to Trade (TBT) Agreement requires all Members of the World Trade Organization (WTO) to notify technical regulations and conformity assessment procedures, when they are not in accordance with the technical content of relevant international standards or if such standards do not exist, through the WTO Secretariat to the other WTO Members. This allows other WTO Members to become acquainted with new product requirements and to comment on them in case they are not in compliance with the TBT Agreement. It also allows an exchange of views to be initiated with the authorities of third countries before the adoption of the measure, which can lead to a modification or even a withdrawal of the proposal. In order to facilitate this, the WTO publicizes a list of National Inquiry Points²¹.

¹⁸ WTO Agreement: www.wto.org/english/tratop_e/tbt_e/tbtagr_e.htm

¹⁹ The TBT agreement is a substantial document and therefore is not repeated in these guidelines. However the full text may be found at: www.wto.org/english/docs_e/legal_e/17-tbt.pdf. Articles 5 through 9 of the agreement deal specifically with “Conformity with Technical Regulations and Standards”, and Article 12 deals with “Special and Differential Treatment of Developing Country Members”.

²⁰ Adapted from JETRO/JISC Inquiry Point: www.jisc.go.jp/eng/wto-tbt/

²¹ National Inquiry Points in TBT Agreement: www.wto.org/english/docs_e/legal_e/17-tbt.pdf

3.3 List of ICT equipment requiring conformity assessment

Standards and conformity assessment can apply to the following types of equipment²²:

- **Radio apparatus:** A device or combination of devices intended for, or capable of being used for, radiocommunication (includes a broad range of equipment from remote car alarms to high-powered broadcast transmitters).
- **Interference-causing equipment:** Any device, machinery or equipment, other than radio apparatus, that can cause interference to radiocommunication (includes digital equipment that uses a microprocessor or microcontroller, and industrial, scientific and medical equipment such as switching power supplies used in halogen lamps).
- **Radio-sensitive equipment:** Any device, machinery or equipment, other than radio apparatus, that can be adversely affected by radiocommunication emissions (includes consumer electronics and industrial controls).

Two categories of equipment may be defined:

Category I: Equipment must meet technical standards and requires a Technical Acceptance Certificate (Certification) in certain countries.

A non-exhaustive list of such equipment would include:

- Broadcasting transmitters
- Portable radio transmitters
- Digital scanner receivers
- Remote car alarms and starters
- Garage door openers
- Wireless computer links
- Cellular phones
- Cordless phones
- Fax machines
- GSM telephones
- Mobile radios
- Modems
- Wireless remote devices
- PABXs (including small business systems and key systems)
- Pagers
- Radio receivers
- Radio transmitters
- Telephone instruments
- Telex equipment

²² 15. Categories of radiocommunication equipment: www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf01698.html

- Other equipment emitting a radio signal
- Any customer premises equipment to be attached to any part of a licensed telecommunication network

Category II: Equipment must meet technical standards but does not have to be certified in certain countries.

This applies to equipment such as: electronic transformers or ballasts, alarm keypads, intelligent battery chargers, satellite TV receivers, VCRs, and computers.

4 Accreditation, recognition and acceptance of laboratories and qualified professional

4.1 Designation/recognition of accreditation and certification bodies, and testing laboratories

Appointment and peer assessment of accreditation bodies

Accreditation is the third-party attestation related to a conformity assessment body conveying formal demonstration of its competence to carry out specific conformity assessment tasks. An accreditation body is an authoritative body that performs accreditation. The authority of an accreditation body is generally derived from government and an accreditation body is usually appointed by the regulatory authority. It is recommended that an appointed accreditation body meets the requirements of ISO/IEC 17011. Internationally the proof of competence with ISO/IEC 17011 is done by peer assessment.

The International Laboratory Accreditation Cooperation (ILAC)²³ is the organization which organizes and conducts peer assessment of accreditation bodies which accredit testing laboratories. Accreditation bodies which are successful in the peer assessment will become signatories of the ILAC Mutual Recognition Arrangement (ILAC MRA)²⁴. ILAC recognizes signatories of the following regional cooperation bodies, the European cooperation for Accreditation (EA)²⁵, the Asia Pacific Laboratory Accreditation Cooperation (APLAC) and the Inter-American Accreditation Cooperation (IAAC).

The International Accreditation Forum (IAF)²⁶ is the organization which organizes and conducts peer assessment of accreditation bodies which accredit certification bodies. Accreditation bodies which are successful in the peer assessment will become signatories of the IAF Multilateral Recognition Arrangements (IAF MLA)²⁷. The IAF MLA relies heavily on the MLA of the three regional accreditation groups; the European co-operation for Accreditation (EA), the Pacific Accreditation Cooperation (PAC)²⁸ and the Inter-American Accreditation Cooperation (IAAC), as it is these groups which perform the majority of the peer evaluation activity not the IAF.

²³ www.ilac.org/

²⁴ <https://www.ilac.org/ilacarrangement.html>

²⁵ www.european-accreditation.org/

²⁶ www.iaf.nu/

²⁷ www.iaf.nu/articles/IAF_MLA/14

²⁸ www.apec-pac.org/

Designation/recognition of certification bodies

It is recommended that the first step for a certification body to complete the designation/recognition process is to get accreditation by an accreditation body to meet ISO/IEC 17065 requirements.

For mandatory requirements, the certification body will submit the results of its accreditation along with administrative and other information to its regulator for designation. If the scope of accreditation covers requirements of a foreign country and the regulator is engaged in an MRA with that foreign country, the regulator after its designation of the certification body will send the same information to the regulator of its MRA partner for recognition.

For voluntary requirements, the certification body will submit the results of its accreditation along with other information to its clients, which would include service providers, associations etc. for recognition.

With successful designation/recognition, the certification body will be able to certify ICT equipment to meet the mandatory requirements and the requirements of its clients.

Designation/recognition of testing laboratories

It is recommended that the first step for a testing laboratory to complete the designation/recognition process is to get accreditation by an accreditation body to meet ISO/IEC 17025 requirements.

For mandatory requirements, the testing laboratory will submit the results of its accreditation along with administrative and other information to its regulator for designation. If the scope of accreditation covers requirements of a foreign country and the regulator is engaged in an MRA with that foreign country, the regulator after its designation of the testing laboratory will send the same information to the regulator of its MRA partner for recognition.

For voluntary requirements, the testing laboratory will submit the results of its accreditation along with other information to its clients which would include service providers, associations etc. for recognition.

With successful designation/recognition, the testing laboratory will be able to test ICT equipment to meet the mandatory requirements and the requirements of its clients.

4.2 Recommendations on policies and strategies for developing conformity assessment testing laboratories compliant with international standards

The following are recommendations on policies and strategies for developing testing laboratories compliant with ISO/IEC 17025.

Legal status/legal entity

The testing laboratory has to be established as an entity that can be held legally responsible for its activities.

Financial policy

Start-up cost includes building, infrastructure development, and procurement of equipment. It is difficult especially in developing countries to cover operating costs from earned income. One of the important tasks will be to develop plans to secure both medium and long term funding for the testing laboratories. One potential source of funding is from government. A commitment from government especially in developing countries to provide long term financial support is a prerequisite in the effort to building a testing laboratory.

Management structure

There is a need to establish a procedure to ensure that departments of a testing laboratory with conflicting interests do not adversely influence compliance with ISO/IEC 17025. For example the finance, administration, quality assurance, IT, the safety officer, and human resources departments do not report to the laboratory management department.

Personnel

It is essential to recruit staff members who have both theoretical training and adequate practical experience. It may be necessary to deploy staff for an extended period of time in a working laboratory in order to gain experience and to maintain their necessary skill set.

Remuneration of staff is an important financial issue. The testing laboratory should have adequate funds in its budget to ensure that fully trained staff is paid well enough in order to keep them in the organization.

Training system

Training is an important part of the laboratory plan and programme. A training programme has to be put in place to train new staff and to keep staff up to date with technological change and evolution.

Premises

There are a number of tasks in the planning and development of the testing laboratory premises, including:

- The selection of test site location is an important issue to be considered. For example an open area test site (OATS) should be located in an electronic “quiet” area in order to minimize electronic interference.
- One of the important tasks in the planning and development of the laboratory premises is the effective separation between neighbouring areas where the activities of these areas are incompatible.
- An example is the separation of wire line and wireless test stations. Another example is the separation of office and laboratory spaces.
- Access to test and calibration areas shall be strictly controlled and limited to authorized personnel. An example of access control is the use of ID cards.
- The location of windows of the building housing the laboratory is an important factor in the design of the building. Proper orientation of the windows of the building is necessary to avoid direct sunlight in order to protect sensitive test equipment. For example in the northern hemisphere, the windows should be located on the north side of the building.
- Environmental control is an important factor. There should be a long term plan for environmental control. For example for the testing of telecommunication equipment, the building temperature should be kept between 15 to 30 degrees Celsius and the relative humidity should be less than 70 per cent.
- Continuity of electricity supply has to be maintained. Uninterrupted power supplies have to be deployed if necessary. Electricity supply variance can affect test equipment and thereby have effects on test results. Voltage stabilizers are required if the voltage variance is greater or less than 5 per cent.

Equipment

Test equipment is an important tool and asset of the testing laboratory. It is important that proper studies and decisions are made before the purchasing of test equipment which has to conform to specifications relevant to the tests being offered by the testing laboratory.

The availability of maintenance and technical support from the supplier/manufacturer of the equipment is an important issue to be considered in the process to select the suppliers for the equipment.

Price is not the only deciding factor to be considered when buying test equipment. It is much better to buy a slightly more expensive equipment for which maintenance is available than a less expensive option for which there is no technical support, in the country or in neighbouring countries.

The criteria to be considered when selecting an equipment vendor include:

- the vendor equipment meets the required specifications;
- the vendor has a leading position in the market place;
- the design, development and manufacture of the equipment take place in a quality system environment such as ISO 9001;
- the vendor provides installation, familiarization and training services; and
- the vendor provides phone and on-site support in local language.

The following steps are necessary in the installation and documentation of equipment:

1. Verify that the location where the equipment is being installed meets the environmental specifications as defined by the equipment vendor.
2. Install the equipment hardware according to the vendor specifications.
3. Install software and start-up according to the vendor specifications.
4. Document the hardware and software being installed including vendor name, model number, serial number and location of installation.

After installation, equipment should be tested for calibration and for performance verification and the steps to be followed include:

1. Develop test procedures and test protocols.
2. Define acceptance criteria based on documented specifications.
3. Ensure that the test engineers have the appropriate qualifications.
4. Perform tests and document test results.
5. Label equipment with status, dates of last and next calibration.
6. Maintain records of calibration and checks.

4.3 Recommendations on how to become accredited by international accreditation bodies (ILAC, IAF, APLAC, IECEE, etc.) in the relevant ICT scope

An important task in the establishment of a testing laboratory compliant with ISO/IEC 17025 is to obtain accreditation of the testing laboratory to meet ISO/IEC 17025 by an accreditation body, which is compliant with ISO/IEC 17011. The International Laboratory Accreditation Cooperation (ILAC) is the organization that organizes and conducts peer assessment of accreditation bodies that accredit testing laboratories.

Similarly an important task in the building of a certification body compliant with ISO/IEC 17065 is to obtain accreditation of the certification body to meet ISO/IEC 17065 by an accreditation body that is compliant with ISO/IEC 17011. The International Accreditation Forum (IAF) is the organization that organizes and conducts peer assessment of accreditation bodies that accredit certification bodies.

The criteria to be considered in the selection of an accreditation body include:

- language;
- proximity to the country if an in-country accreditation body is not available;

- accreditation cost which can vary between different accreditation bodies - the cost will also depend on the assessors employed for the accreditation and the scope of the accreditation;
- for testing laboratory, accreditation body is a signatory to ILAC MRA or a member of regional cooperation bodies recognized by ILAC;
- for certification body, accreditation body is a signatory to IAF MLA or a member of regional cooperation bodies recognized by IAF.

The testing laboratory or certification body should create a team with a team leader to:

- define the scope of accreditation;
- learn the ISO/IEC 17025 requirements for testing and ISO/IEC 17065 for certification;
- conduct gap analysis and subsequently prepare a task list to resolve the deficiencies;
- estimate costs;
- obtain management decision.

Once decision is made to go ahead, the testing laboratory or certification body should create a team to obtain accreditation and the steps include:

1. The selection of an accreditation body.
2. The development of documentation for the accreditation process.
3. Training of staff.
4. Internal audit and corrections.
5. Pre-assessment and corrections.
6. Accreditation audit.

Long term financial and managerial support is necessary to maintain accreditation and the testing laboratory or certification body should have the necessary processes in place to obtain and maintain financial and managerial support.

References

- Canadian Telecommunications Act: [http://en.wikipedia.org/wiki/Telecommunications_Act_\(Canada\)](http://en.wikipedia.org/wiki/Telecommunications_Act_(Canada))
- Canadian Spectrum Management and Telecommunications Regulations: www.ic.gc.ca/eic/site/smt-gst.nsf/eng/home
- Guidance on European Commission R&TTE Directive: <http://ec.europa.eu/enterprise/sectors/rtte/documents/guidance/>
- ITU SG 11 TD GEN 0256 Draft Technical Report on Counterfeit Equipment: www.itu.int/md/T13-SG11-131107-TD-GEN-0256/en
- OECD ICCT Product Classification Report: www.oecd.org/sti/ieconomy/2771160.pdf
- International Numbering Plans: www.numberingplans.com/?page=analysis&sub=imeinr
- Unique ID Coding: www.uidcenter.org/learning-about-ucode
- ITU-T Recommendation F.771 Service description and requirements for multimedia information access triggered by tag-based identification.
- PP 10 Resolution 177: www.itu.int/ITU-D/tech/NGN/ConformanceInterop/PP10_Resolution177.pdf
- Guidelines for Developing Countries for Establishing Test Labs: www.itu.int/ITU-D/tech/ConformanceInteroperability/ConformanceInterop/Guidelines/Test_lab_guidelines_EV8.pdf
- Technical Requirements for Radio Systems: www.ic.gc.ca/eic/site/icgc.nsf/eng/06957.html#q=srsp
- Safety Code 6 and SAR: www.c4st.org/safety-code-6
- WTO Agreement: www.wto.org/english/tratop_e/tbt_e/tbtagr_e.htm
- National Inquiry Points in TBT Agreement: www.wto.org/english/docs_e/legal_e/17-tbt.pdf
- Categories of radiocommunication equipment: www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf01698.html
- WTO TBT Agreement: www.wto.org/english/docs_e/legal_e/17-tbt.pdf
- Adapted from JETRO/JISC Inquiry Point: www.jisc.go.jp/eng/wto-tbt/
- ISO 6346 Freight containers -- Coding, identification and marking.
- ITU-T Recommendation F.771 Service description and requirements for multimedia information access triggered by tag-based identification.
- Plenipotentiary Conference of the International Telecommunication Union (Guadalajara, 2010): www.itu.int/ITU-D/tech/NGN/ConformanceInterop/PP10_Resolution177.pdf
- ITU report on conformity and interoperability assessment on a regional basis, Southern African Development Community (SADC): www.itu.int/en/ITU-D/Technology/Documents/ConformanceInteroperability/SADC%20Assessment%20Study_Final_November13.pdf
- ITU-T Recommendation X.668: Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: Registration of object identifier arcs for applications and services using tag-based identification
- WTO committee on conformity assessment: www.wto.org/english/tratop_e/tbt_e/tbt_wrkshop_note_21march05_e.doc

International Telecommunication Union (ITU)
Telecommunication Development Bureau (BDT)
Office of the Director
Place des Nations
CH-1211 Geneva 20 – Switzerland
Email: bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Deputy to the Director and
Director, Administration and
Operations Coordination
Department (DDR)
Email: bdtdeputydir@itu.int
Tel.: +41 22 730 5784
Fax: +41 22 730 5484

Infrastructure Enabling
Environment and
e-Applications Department (IEE)
Email: bdtiee@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

Innovation and Partnership
Department (IP)
Email: bdtip@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

Project Support and Knowledge
Management Department (PKM)
Email: bdtpkm@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

Africa

Ethiopia
International Telecommunication
Union (ITU)
Regional Office
P.O. Box 60 005
Gambia Rd., Leghar ETC Building
3rd floor
Addis Ababa – Ethiopia

Email: itu-addis@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, 3^e 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
19, Rue Parchappe x Amadou
Assane Ndoye
Immeuble Fayçal, 4^e étage
B.P. 50202 Dakar RP
Dakar – Senegal

Email: itu-dakar@itu.int
Tel.: +221 33 849 7720
Fax: +221 33 822 8013

Zimbabwe
International Telecommunication
Union (ITU)
Area Office
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792 Belvedere
Harare – Zimbabwe

Email: itu-harare@itu.int
Tel.: +263 4 77 5939
Tel.: +263 4 77 5941
Fax: +263 4 77 1257

Americas

Brazil
União Internacional de
Telecomunicações (UIT)
Regional Office
SAUS Quadra 06, Bloco "E"
11^o andar, Ala Sul
Ed. Luis Eduardo Magalhães (Anatel)
70070-940 Brasília, 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 0343/4
Fax: +1 246 437 7403

Chile
Unión Internacional de
Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Casilla 50484, Plaza de Armas
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 Palmira, Avenida Brasil
Ed. COMTELCA/UIT, 4.º piso
P.O. Box 976
Tegucigalpa – Honduras

Email: itufegucigalpa@itu.int
Tel.: +504 22 201 074
Fax: +504 22 201 075

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: itucairo@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

Asia and the Pacific

Thailand
International Telecommunication
Union (ITU)
Regional Office
Thailand Post Training Center, 5th
floor,
111 Chaengwattana Road, Laksi
Bangkok 10210 – Thailand

Mailing address
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210 – Thailand

Email: itubangkok@itu.int
Tel.: +66 2 575 0055
Fax: +66 2 575 3507

Indonesia
International Telecommunication
Union (ITU)
Area Office
Sapta Pesona Building, 13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10001 – Indonesia

Mailing address:
c/o UNDP – P.O. Box 2338
Jakarta 10001 – Indonesia

Email: itujakarta@itu.int
Tel.: +62 21 381 3572
Tel.: +62 21 380 2322
Tel.: +62 21 380 2324
Fax: +62 21 389 05521

CIS countries

Russian Federation
International Telecommunication
Union (ITU)
Area Office
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

Mailing address:
P.O. Box 25 – Moscow 105120
Russian Federation

Email: itumoskow@itu.int
Tel.: +7 495 926 6070
Fax: +7 495 926 6073

Europe

Switzerland
International Telecommunication
Union (ITU)
Telecommunication Development
Bureau (BDT)
Europe Unit (EUR)
Place des Nations
CH-1211 Geneva 20 – Switzerland
Switzerland
Email: eurregion@itu.int
Tel.: +41 22 730 5111



International Telecommunication Union
Telecommunication Development Bureau
Place des Nations
CH-1211 Geneva 20
Switzerland
www.itu.int