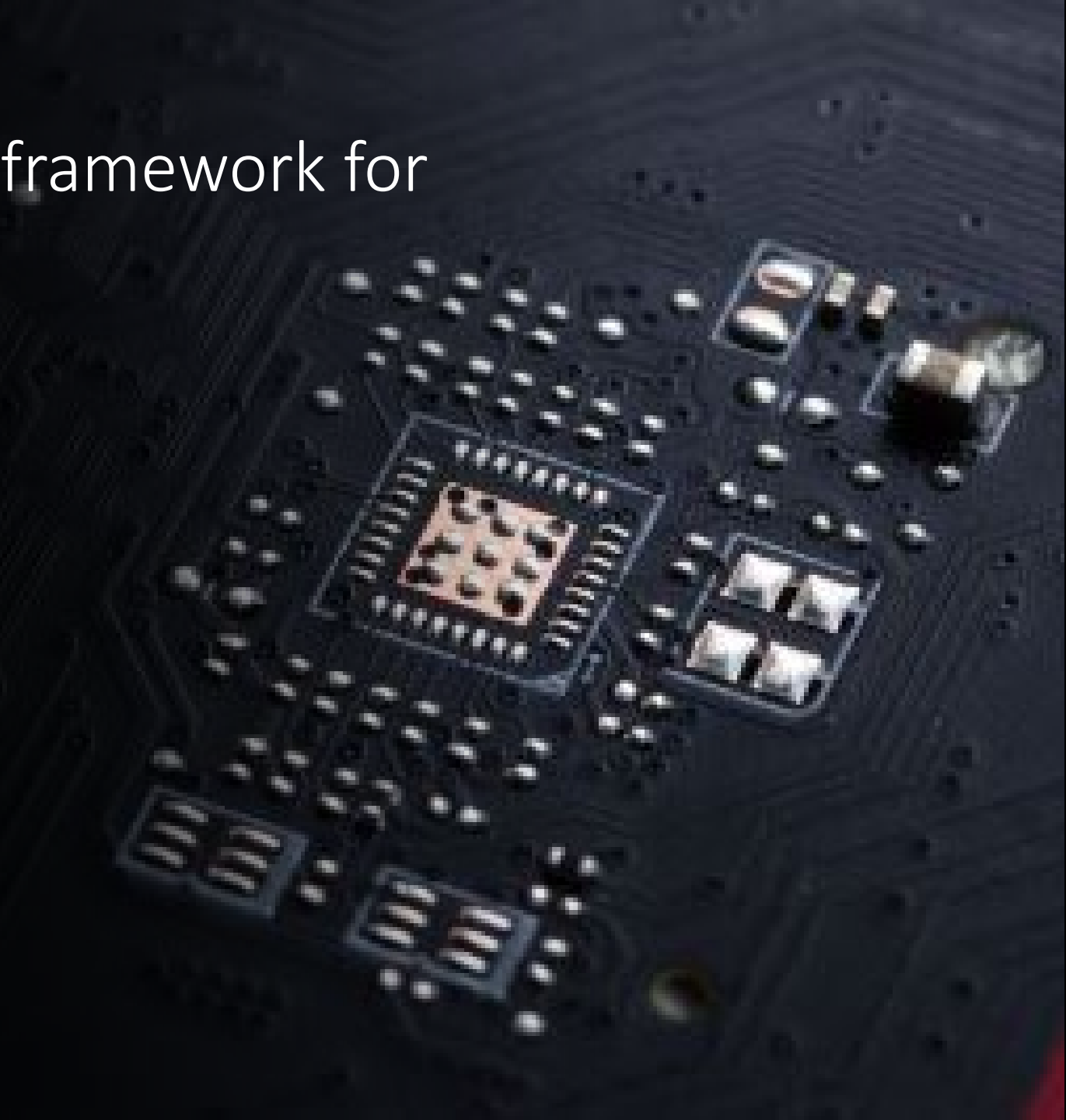




New conformity assessment framework for telecommunication products Brazil

- Law and Regulation
 - New Framework
 - Technical and Operational requirements
 - Cybersecurity framework
 - Market Surveillance
-



Applicable Law and Regulation

Law 9.472 – General Telecommunications Mark

- Establishes that Anatel, the Brazilian National Telecommunications Agency is responsible for issuing or recognizing the certification of telecommunication products and for issuing standards and regulations regarding their use in Brazil.

July 1997

Nov. 2000

Resolution 242 – General regulations for Certification and Approval of telecommunication products

- Establishes that any telecommunication product, before it may be sold or used in Brazil, must have a CERTIFICATE OF CONFORMITY issued by a Designated Certification Organization – OCD and HOMOLOGATED (APPROVED) by Anatel.

OCD: brazilian certification body

Applicable Law and Regulation



Anatel Resolution 242 (2000)

- First assessment framework of telecommunication product;
- Classifies the types of products into categories according to destination (user) and telecommunications service;
- Single conformity assessment model per type approval.



Anatel Resolution 715 (2019)

- Establishes a new assessment framework for any telecommunication product for the Brazilian Market;
- Flexibility on conformity assessment model;
- Products are no longer divided into main categories;
- Defines Market Surveillance process.

ALMOST 2 DECADES

Applicable Law and Regulation



PRINCIPLES FOR PRODUCT ASSESSMENT CONFORMITY

SPECTRUM AND NETWORK PROTECTION

TECHNOLOGY DEVELOPMENT

USER SAFETY

EFFICIENT AND RACIONAL SPECTRUM USE

INTEROPERABILITY

QUALITY AND DURABILITY

ENVIRONMENT

ECONOMIC AND COPETITIVE FREEDOM



New Framework



New framework created by Resolution 715 is intended to bring greater flexibility in the process.



Establishment of technical requirements by a simple process:

Rules are discussed with stakeholders involved;
Rules are approved by a simple process: They are approved by an act issued by the superintendent.



All operational procedures (assessment modality, documents,..) also are established by a simple process, like a technical requirements.



Improve the post-marketing surveillance process.

New Framework

Five pillars



New Framework

Models of Conformity Assessment Program (CAP)

Certification by OCD (type approval test)

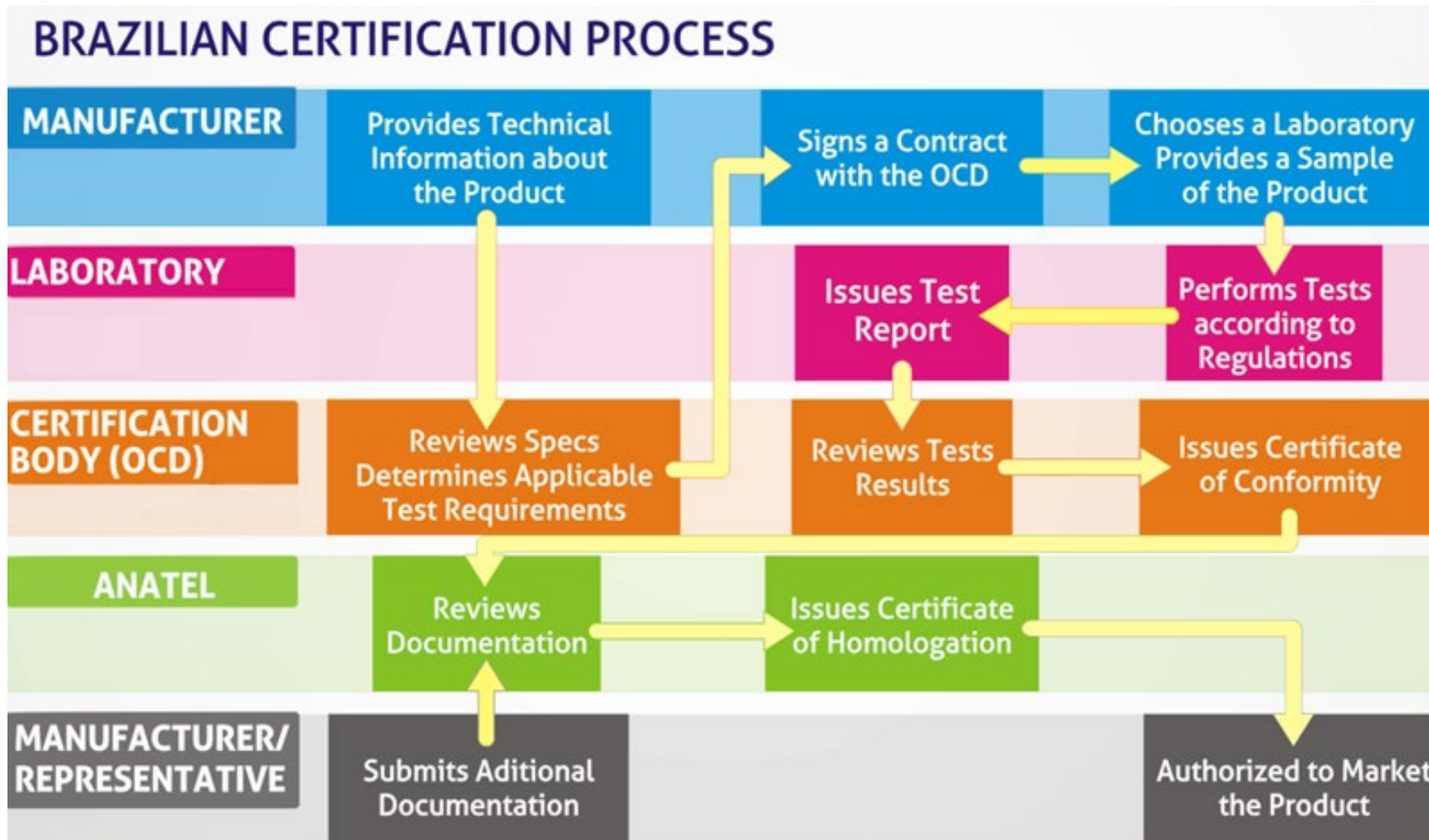
Periodic Maintenance
of Certification

Manufacturing Quality
Management
(ISO Standards)

- > Product intended for citizens normally devoid of technical knowledge;
- > Transmitter and transceiver RF products;
- > Critical operations.



Conformity Assessment – Certification



New Framework

Models of Conformity Assessment Program (CAP)

Declaration of Conformity (DoC)

Declares the compliance of technical standards issued by Agency

Manufacturing Quality Management (ISO Standards)
(commercial purpose)

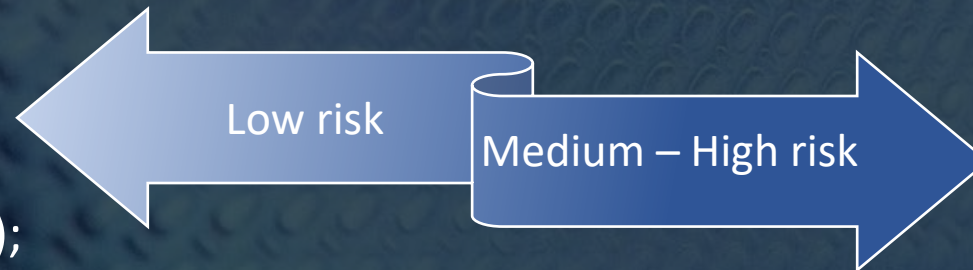
- > Intended for special applications and with low scale of manufacturing production;
- > Must keeping laboratory test to prove the complies with technical standards when request and before commercial distribution or to owner use purposes.
- > Direct approval with the Agency.

New Framework

- 63 products are approved upon a **DoC**:

[Approved by Anatel Act no. 7280 of November 26, 2020](#)

- Data multiplex;
- Data network equipment;
- Cable connectors;
- Optical Distribution Frames (e.g. splitters);
- Aeronautical & Marine services;
- P2P Antennas;
- (...)



- 103 products are maintained to be approved upon 3rd party **Certification**:
 - Mobile phones;
 - Battery and power supplies for mobile phones;
 - Terminal equipment (CPE);
 - Short Range Devices;
 - Fixed and mobile radios for private a public networks;
 - Base Station;
 - Microwave radios;
 - (...)
- Extension of periodic evaluation of technical requirements to 2~3 years.

Technical and Operational Requirements

Anatel establishes which types of products are subject to mandatory Certification.

Anatel publishes the list of technical requirements and test procedures for certification of telecom products (Performance, EMC and Safety).

The old standards and regulations are being replaced or updated to include new types of products and new technologies.

Electromagnetic Compatibility,
Electrical Safety requirements and
SAR.

Wireless equipments requirements
(e.g. 5G cell phones, WiFi, BT, others SRD).

Performance requirements
(e.g IPv6 connectivity and product durability).

Cybersecurity recommendations.

Technical and Operational Requirements

Production chain and the IoT ecosystem

High demand for connected devices;
Fast growth in equipment approvals;
New ways to provide/use connectivity (5G, IoT).

Specific operational procedure for assessment of ICT products who embedded 3rd party RF modules.

Relationship with other government conformity assessment programs of country for non ICT products.
(e.g.: electromedical equipment, industrial and home appliance, and others)

Procedure for monitoring software and hardware modifications for embedded RF modules on ICT and non ICT devices after certification approval.



Technical and Operational Requirements

Software updates in telecommunication products

Manufacturers release software updates to fix and upgrade features in products.

May have new functionalities, like new operations modes, frequency ranges, etc.

By regulations established by Anatel, the manufacturer or your legal representative in Brazil need to inform the OCD about all features released in the software update.

- If some feature needs to be recertified, the OCD (certification body) will inform all tests and documentations necessary.

Cybersecurity Framework - Overview

- Vulnerabilities in telecommunications equipment's are reported every day.
- Conformity assessment process normally is a “deterministic process”.
 - Ex.: Power radiated requirements, maximum output power, etc.
- Vulnerabilities may be embedded intentionally in:
 - Software – Malwares, virus, etc.
 - Configurations – standard credentials, use of obsolete and insecure protocols, etc.
- Some vulnerabilities are unintentional
 - Backdoors resulting from hardware or program code design flaws.





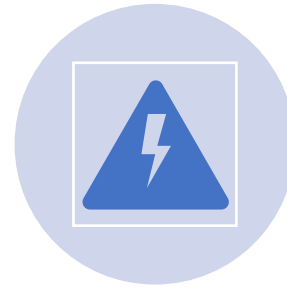
Cybersecurity Framework

- Established by [Anatel Acts no. 77 of January 5, 2021](#) and [no. 2436 of March 7, 20213](#).
- It is intended to establish a set of cybersecurity recommendations covering all; telecommunications products approved by Anatel that connect to the internet and equipment for provider's network;
- The main objective is to reduce the risk of the user and the telecommunication networks;
- Currently, it is not mandatory for equipment approval.

Cybersecurity Framework



All telecommunications equipment must be certified and approved by Anatel and the cybersecurity recommendation (Act. 77/21) are not mandatory;



Products undergo laboratory tests to assess whether they meet requirements defined by Anatel (performance aspects, electrical safety, electromagnetic compatibility, specific absorption rate, etc.). After these tests, the manufacturer declares which recommendation of cybersecurity the product complies;



The approval must be renewed every 2 years to prove that the product continues to meet the requirements assessed in its initial certification;



Products can be submitted to market surveillance tests at any time to assess whether the homologated product and its supplier are in conformity with manufacturer declares.


Cybersecurity Framework

- Based on best practices, recommendations and internationally recognized frameworks:
 - IETF - Internet of Things (IoT) Security: State of the Art and Challenges - RFC 8576.
 - LAC-BCOP-1 (May/2019) – Best Current Operational Practices on Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition.
 - ENISA - Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures.
 - GSMA IoT Security Guidelines – Complete Document Set.
 - ETSI GS NFV-SEC 001 V1.1.1 (2014-10) - Network Functions Virtualisation (NFV); NFV Security; Problem Statement.
 - ISO/IEC 27402 — Cybersecurity — IoT security and privacy — Device baseline requirements [DRAFT].
 - Common Vulnerability Scoring System (CVSS), acessível em: <https://www.first.org/cvss>.
 - ETSI EN 303 645 v2.1.1 (2020-06) - CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements.
 - ETSI TS 133 117 V16.5.0 (2020-08) - Universal Mobile Telecommunications System (UMTS); LTE; Catalogue of general security assurance requirements.



Market Surveillance Program

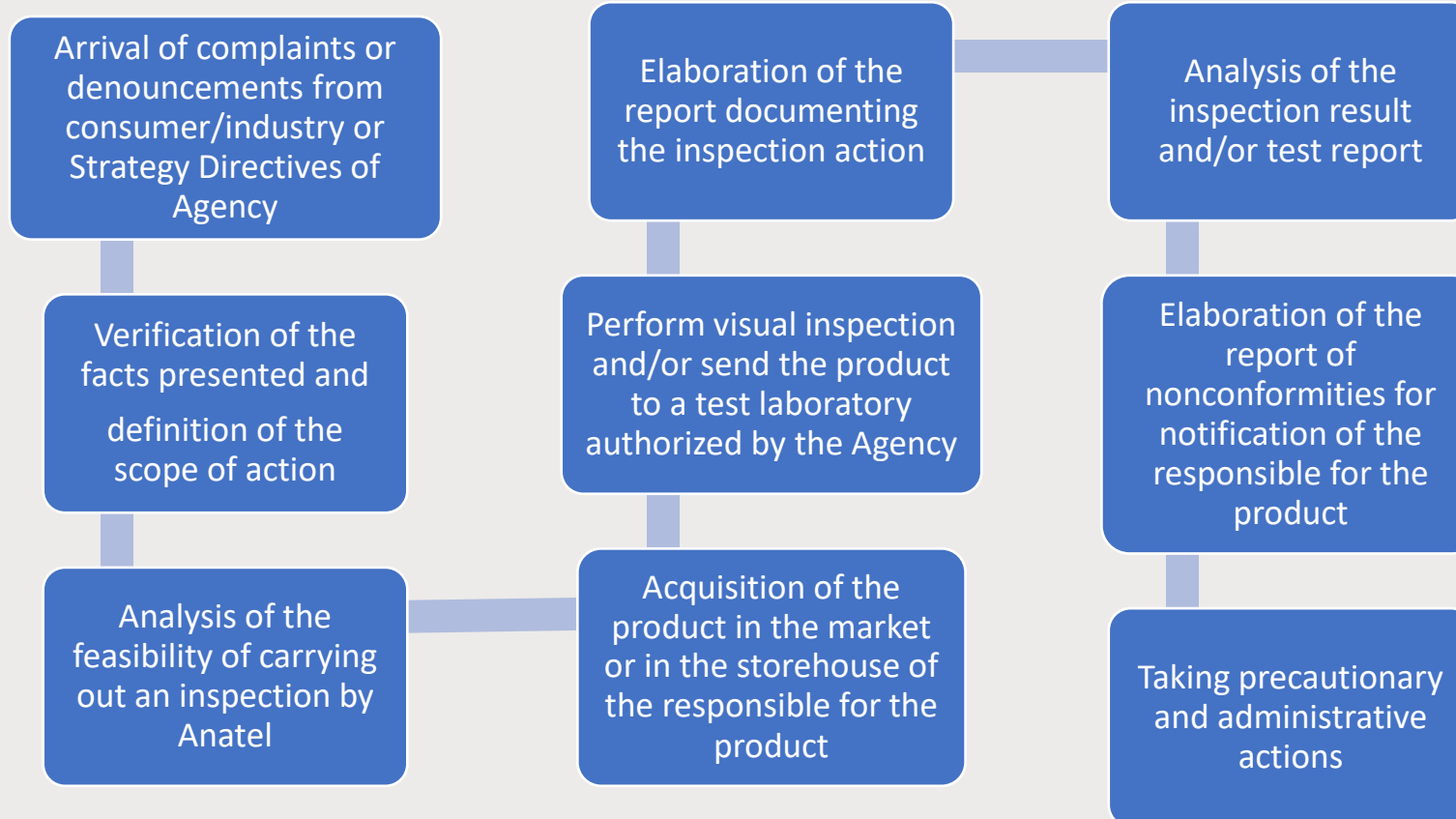
- General provisions for a market oversight;
- Applied to overall products approved by the Agency;
- Samples collected at market or at the manufacturing or storehouse premises.
- Carried out based on complaints or denouncements from consumers and industry or anytime by Agency whenever they identify the relevant one.
- The certificate owner is responsible for the market surveillance costs.
- Prevision of a product recall to be performed by manufacturer or local representative.



Cybersecurity Surveillance (Act no. 77/21)

- Intends to evaluate whether the product meets the security recommendations declared by the manufacturer at the time of its approval;
- Search for any cybersecurity flaw in the product;
- Depending on the cybersecurity vulnerability found in the product, its approval is suspended;
- If the manufacturer does not fix the vulnerability, the product approval also may be canceled.

Market Surveillance - Overview



Conclusions



Conformity assessment may be an important tool to protect and reach an efficient use of spectrum, beyond to help improve a security in provider networks and user environment;



It's important to note that some cybersecurity vulnerabilities may be present intentionally or non intentionally;



Market surveillance is an important tool to discovery and fix manufacturing flaws and to establish recall programs;



Most important: digital transformation create new challenges of C&I programs around the world and collaboration with other actors and members of state is essential to deal with the problem.