COMPLIANCE UPDATE

Monthly Newsletter

VOL.07 JULY 2025

Global Compliance News

Australia

Upcoming Changes to the Cellular Standards

New versions of the Australian cellular standards AS/CA S042.1, S042.4, and S042.5 are expected to be published soon. Following their publication, there will be a 12-month transition period during which equipment may be tested or assessed to either of the 2022 or 2025 standards.

So, what's new in AS/CA S042.1:2025?

The S042.1 standard primarily covers requirements for emergency dialing and acoustic safety. The major change to the 2025 version is the inclusion of Emergency Cell Broadcast requirements for the upcoming National Messaging System (NMS). This system is based largely on the existing European (EU-Alert) and North American requirements and is expected to be active in mid-2027.

What does this mean for my product?

We would expect most mobile phones to already be compliant with EU-Alert requirements, so there shouldn't be much more needed here. The Australian standard puts in additional requirements to EU-Alert such as alert tones based on the North American rules, and how information is presented to the user.

For now, you only need to provide a declaration to the relevant European and North American rules, as well as our Australian additions.

What's new in AS/CA S042.4:2025 and AS/CA S042.5:2025

The big change to S042.4:2025 is the removal of 3G (UMTS) requirements. With the shutdown of 3G by all telecommunication providers in Australia, this section is no longer relevant. S042.4:2025 also adds requirements for Non-Terrestrial Networks (NTN), though no requirements for emergency calls or alerts over NTN are introduced.

With the publication of the European harmonised standard for 5G NR (EN 301 908-25), the S042.5:2025 standard incorporates new requirements based on this. As with previous versions of the S042 standards, if your product is compliant in Europe, it's very likely to be compliant in Australia.

The new standards also include requirements for band 26, which was recently implemented by Australian networks due to its crossover with existing band 5. Being a North American band, our requirements are based on FCC rules.

Australia
AS/NZS 62368.1:2022 Standard Adopted

On June 24, 2022, the new standard AS/NZS 62368.1:2022 (Safety Requirements for Audio, Video, Information and Communication Technology Equipment) was released. This standard sets a transition period of 3 years and was enforced on June 24, 2025, officially replacing the old standard AS/NZS 62368.1:2018.

AS/NZS 62368.1:2022 is based on IEC 62368-1:2018 3rd edition, and the IECEE website has published its Australian national differences for CB certification use.

Industry Canada Industrie Canada

Canada
New Radio Standard RSS-193

The Canadian communications regulator Industry Canada under the Science and Economic Development Canada (ISED) has officially published a new Radio Standard RSS193 Issue 1.

RSS193 Issue 1 introduces certification requirements for flexible use broadband equipment operating in the 27.5–28.35 GHz frequency band.

RSS-193 Issue 1 outlines the technical and procedural requirements for the certification of equipment used in fixed and/or mobile services within the 27.5 to 28.35 GHz spectrum. This frequency band is especially significant in supporting flexible use broadband services, including advanced 5G deployments and innovative high-frequency communication applications.

The specification applies to equipment intended for:

·Fixed broadband service
·Mobile broadband service
·Future technologies utilizing high-band 5G frequencies

A.R.C.T.

Burundi
Updates to Equipment Certification Rules

The Burundi regulator ARCT has just announced updates to it Regulation for Radio Equipment and Terminal Devices.

This latest announcement means that all radio equipment and terminal must be approved by ARCT and properly labelled with both ARCT and customs (OBR) stickers.

The agence de Régulation et de Contrôle des Telecommunications (ARCT) of Burundi has introdcued the new rules Ministerial Order No. 580/01 on April 17, 2025, to control the import, sale, and distribution of telecommunications and ICT equipment. From now on, all devices must be approved by ARCT and properly labeled with both ARCT and customs (OBR) stickers.

The labeling will be handled locally by ARCT, OBR, and the national standards body (BBN).

Europe

Cybersecurity Radio Equipment Directive. Are you Ready?

From 1st August 2025, all wireless devices placed on the EU market must comply with the Radio Equipment Directive (RED) cybersecurity requirements.

As more products have integrated wireless radio interfaces in their applications. Many of these devices connected to the internet potentially face security risks, making them vulnerable to potential attacks and exploitation. To mitigate these risks, the European Commission adopted a Delegated Act of the Radio Equipment Directive activating Articles 3(3)(d), (e) and (f) for certain categories of radio equipment to increase the level of cybersecurity, personal data protection and privacy, and protection of financial transactions.

·Article 3.3 (d) - radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service.
·Article 3.3 (e) - radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected.
·Article 3.3 (f) - radio equipment supports certain features ensuring protection from fraud

So what kind of devices are subject to the RED Cybersecurity requirements?

1.Equipment that uses radio technology for communication over the internet such as mobile phones, tablets, electronic cameras, telecommunication equipment
2.IoT devices that can transmit data over the internet
3.Toys and childcare equipment such as baby monitors
4.Wearable devices such as smartwatches or fitness trackers
5.Connected industrial devices

How do I demonstrate compliance to the Cybersecurity Requirements?

Compliance with essential requirements is usually achieved by applying standards. The adopted harmonised cybersecurity standard is EN 18031. There are 3 parts to the standard, EN 18031-1:2024 covers essential requirement 3(3)d on network protection. EN 18031-2:2024 covers essential requirement 3(3)e on safeguarding personal data and privacy. EN 18031-3:2024 covers essential requirement 3(3)f on protection from fraud.

You should understand how these standards apply to your products and any restrictions affecting their use. Conduct a Compliance Gap Analysis: Assess your current cybersecurity measures against EN 18031 requirements. Prepare for Market Readiness: Implement necessary changes in design, testing, and documentation to meet the August 2025 deadline.

For further guidance or to discuss your product's certification process, contact us:

Global Certification
Product Labelling Requirements.

One of the key questions we are asked by our partners is regarding the labelling requirements for their products, once product certification is achieved.

As ICM are active in over 180 markets worldwide we have a super understanding of the labelling requirements for products. As part of our management service we provide the labelling information in a timely manner to allow production teams to prepare product labels, ready for the launch of their products. To give you an idea of the countries which have labelling requirements please see the table below:

Algeria	Indonesia	Serbia
Argentina	Japan	Singapore
Australia	Jordan	South Africa
Botswana	Lebanon	South Korea
Brazil	Malaysia	Taiwan
Canada	Mexico	Tanzania
China	Morocco	UAE
Europe	Nigeria	US
Gabon	Oman	Uganda
India	Pakistan	Zambia

For more information please contact markb@internationalcompliancemanagement.com