Position Paper

TIC COUNCIL VIEW OF THE SCOPE OF THE RED DELEGATED ACT AND EN18031 SERIES

29 October 2024

INTRODUCTION - STRENGTHENING DIGITAL TRUST THROUGH ENHANCED CYBERSECURITY

TIC Council, the international trade association representing the testing, inspection, and certification (TIC) industry, welcomes the European Commission's efforts to strengthen the cybersecurity of the Internet of Things (IoT). Secure and trustworthy IoT devices for European consumers are crucial for achieving the Digital Decade targets for 2030[1], strengthening the EU's competitiveness and security, and fostering **Digital Trust**.[2] Therefore, effective implementation and enforcement of EU cybersecurity legislation will be critical.

The 2014/53/EU Radio Equipment Directive (RED) addresses, in addition to other requirements, cybersecurity challenges such as privacy protection, personal data security, and fraud prevention. The 2022/30 RED Delegated Act (RED-DA) outlines the specific cybersecurity requirements radio equipment must meet to be placed in the EU market, in line with *Articles 3(3)(d), (e), and (f) of the RED*. The RED-DA will take effect in August 2025, requiring manufacturers to comply with these essential cybersecurity requirements to be able to place their products in the EU.

However, uncertainties persist regarding the scope of the RED-DA and the EN18031 series for its correct implementation. To address these, TIC Council seeks to provide its view of the scope of the RED-DA and EN 18031 series, drawing on its Members' roles as Notified Bodies (NB) and enablers of Digital Trust.

This position paper reflects a common interpretation shared by TIC Council Members and serves as input for discussions with industry, conformity assessment bodies, and policymakers. It is not intended as legal advice but as a summary of the current state of discussions among TIC Council Members as of October 2024.

RECOMMENDATIONS FOR MANUFACTURERS

1. Adopt a proactive approach to security:

- This is crucial, as manufacturers bear full responsibility for conducting cybersecurity risk assessments for their devices and choosing the appropriate compliance procedures. TIC Council recommends following ETSI's risk management process[3] (see *Figure 1*).
- The cybersecurity risk assessment must be performed early in the development phase and maintained throughout the product's lifecycle to ensure ongoing security.

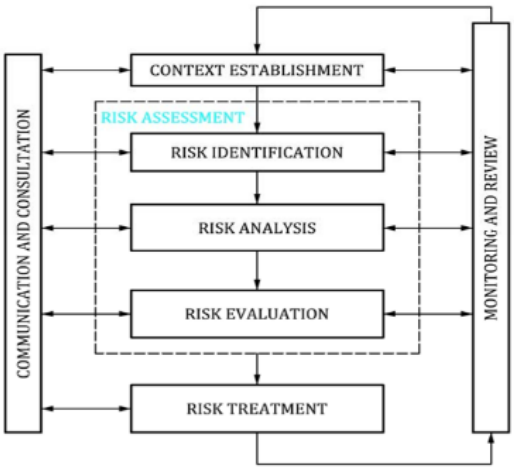

Figure 1: Risk management process in ISO/IEC 27000 series and ISO/IEC 31000 series

[1] Decision (EU) 2022/2481 Establishing the Digital Decade Programme 2030, Official Journal of the EU, 2022, pages 12-13.

[2] For further details, refer to TIC Council's Recommendations on Securing IoT Devices for Consumers.

[3] Cyber Security (CYBER); Assessment of cyber risk based on products' properties to support market placement, European Telecommunications Standards Institute (ETSI), 2023, page 33.

2. Get ready for compliance before the deadline (August 2025):

- If you are unsure how to begin the process or need assistance, seek guidance from your trusted NB well in advance of the transition period's end. This will help you identify any major compliance gaps early on.
- Use well-structured documentation to reduce efforts and costs.
- Monitor the development of the EN 18031 standard series and its publication as a harmonised standard (hEN) by the European Commission as it will provide a-presumption of conformity with the RED-DA.
- Anticipation for compliance is increasingly important as the Cyber Resilience Act (CRA) will set cybersecurity requirements for a broader range of products. TIC Council urges co-legislators to expedite its approval to ensure that products and software with digital components are secure for EU consumers.

3. Become familiar with the conformity assessment procedures under the RED:

- Third-party conformity assessment (*Module B+C or H*)[4]: Manufacturers shall follow these modules in cases where a harmonised standard is not available or when they opt for applying a non-harmonised standard (e.g., based on ETSI EN 303 645).
- Self-assessment of conformity (*Module A*): Manufacturers use this procedure when it applies harmonised standard. Under this case, manufacturers are not obliged to use a NB for the conformity assessment procedure. However, manufacturers are free to choose to involve a NB to strengthen security and ensure compliance. For more information regarding the necessary conformity assessment procedures per aspects of essential requirements of the RED-DA, see *Figure 2*[5].

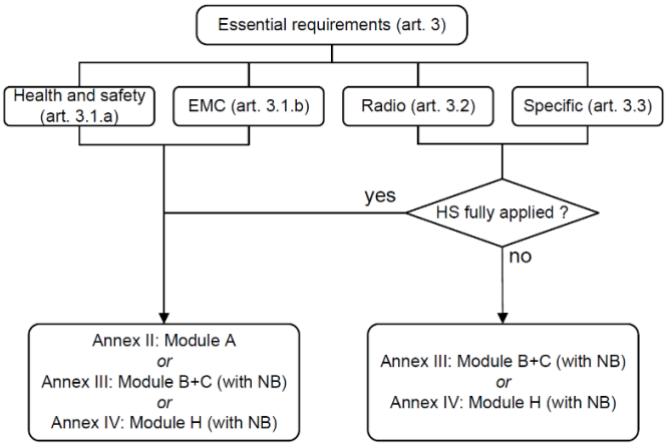

Figure 2: Overview of the different conformity assessment procedures

4. Understand when and how to use harmonised standards:

- When using harmonised standards from the Official Journal of the EU to meet essential requirements laid down in EU legislation, manufacturers must conduct a product-specific risk assessment to identify and address potential risks (this is also valid when the manufacturer is not using harmonised standard for the evaluation).

[4] Note: Module B (EU-type examination procedure for the design phase of development), Module C (conformity to-type procedure based on internal production control - performed by manufacturer) and Module H (full quality assurance procedure for the design and production phases).

[5] Guide to the Radio Equipment Directive 2014/53/EU, page 20, Version of 19 December 2018.

- If the harmonised standard sufficiently addresses all identified risks associated with the device, and the manufacturer chooses to apply them (as per the self-declaration of conformity), they can benefit from the presumption of conformity (see *RED Article 16*)[6].
- However, if any of the identified risks are not covered by the harmonised standard or are not fully applied, the manufacturer must justify and address security measures on how the essential requirements are still fulfilled for those uncovered risks. In this case, involving a NB for the conformity assessment by the manufacturer is required. For further information, see the European Commission's steps to affix a CE marking.[7]

CONSIDERATIONS ON THE SCOPE OF THE RED-DA

1. Lack of guidance on the definition of "Internet-connected radio equipment" in RED-DA Article 1[8]:

- TIC Council considers the term "Internet-connected radio equipment" to be broader than radio equipment that connects itself to the Internet (e.g., implementing TCP/IP protocols). Radio equipment should be considered connected to the Internet if it has any pathway through which data is transmitted to or received from the Internet. This includes instances where data, such as an ID, is sent to the cloud or where information, like firmware updates, is received from the Internet. Any form of communication with the Internet, whether direct or indirect, in any part of the data chain, should fall under this definition.
- Manufacturers must consider the product's intended use and foreseeable usage while conducting the risk assessment. This ensures they accurately assess the risks of non-compliance with the essential requirements outlined in *RED Article 3.3 (d/e/f)*.

2. TIC Council emphasises the importance of aligning the following terms with the corresponding legislative texts:

- "Processing" and "personal data" as defined in the Regulation 2016/679 General Data Protection Regulation (GDPR);
- "Traffic data" and "location data" as defined in the 2002/58/EC e-Privacy Directive;
- "Virtual currency" as defined in the Directive 2019/713 on combating fraud and counterfeiting.

[6] "Radio equipment which is in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the essential requirements set out in Article 3 covered by those standards or parts thereof."

[7] Manufacturers and CE Marking, European Commission (n.d.).

[8] "The essential requirement set out in Article 3(3), point (d), of Directive 2014/53/EU shall apply to any radio equipment that can communicate itself over the internet, whether it communicates directly or via any other equipment ('internet-connected radio equipment')."

CASES SCENARIOS IN THE SCOPE/OUT OF SCOPE

The assessment of whether a device falls within the scope of the RED-DA depends on the device itself, the environment in which it operates, the intended use and the risk assessment.

1. In-scope devices:

- Any device that can communicate itself over the Internet, whether it communicates directly or via any other equipment could fall under the scope of the RED-DA. To determine if a device is subject to the cybersecurity requirements under the RED-DA, manufacturers should conduct a comprehensive risk assessment. This assessment should, as far as possible, consider both the intended and reasonably foreseeable conditions of the device to ensure the highest level of security for consumers, as stressed in Chapter 2.8 on "Reasonably foreseeable and intended use/misuse[9]" of the Blue Guide.
- A recent case involving the Tire Pressure Monitoring System (TPMS) in cars illustrates the critical need for thorough risk assessment. According to a study[10], a vulnerability was identified in the Tesla Model 3's TPMS, which communicates wirelessly via Bluetooth, creating an indirect Internet connection. This flaw enabled attackers to execute malicious code on the vehicle's immobiliser Electronic Control Unit (ECU) by exploiting its communication with other ECUs. Other examples of unintended cyberattacks include the casino fish tank hack,[11] where a smart device was used to infiltrate the network, further highlighting this issue. These cases underscore the importance of conducting in-depth risk assessments to identify potential threats and ensure the highest level of security for consumers.

2. Out-of-scope devices:

- As outlined in Article 2(1)[12] of the RED-DA, the essential requirements do not apply to devices covered by other legislation, such as Regulation 2017/745 on Medical Devices and Regulation 2017/746 on In Vitro Diagnostic Medical Devices (e.g., Wireless Smart Blood Glucose Monitor Kits).

SCOPE OF THE EN18031 SERIES

CEN-CENELEC published the EN 18031 series in August 2024. The European Commission must now decide whether to publish it in the Official Journal of the EU for harmonisation. The EN 18031 includes a decision tree to determine necessary security features based on a product's intended use. This decision tree requires justifications, meaning manufacturers must conduct a cybersecurity risk assessment.

[9] The Blue Guide on the implementation of EU product rules, European Commission, 2022, page 25.

[10] Breach in Tesla Model 3's TPMS Unveils Serious Security Flaw, Cybellum, 12 September 2024.

[11] Odd cyber-attack: Casino fish tank hack, OryxAlign, 14 March 2024.

[12] "By way of derogation from Article 1, the essential requirements set out in Article 3(3), points (d), (e) and (f), of Directive 2014/53/EU shall not apply to radio equipment to which either of the following Union legislation also applies: (a) Regulation (EU) 2017/745; (b) Regulation (EU) 2017/746."

While using EN 18031 (if harmonised) may simplify the compliance process for RED-DA, it should not preclude consideration of alternative paths. Manufacturers can directly apply essential requirements or refer to the European Commission's standardisation request[13] and choose any relevant standard. However, this approach necessitates involvement with a NB and more justifications.

1. Interplay with ETSI EN 303 645[14] and IEC EN 62443 series:

- TIC Council advises careful use of Annex C of EN 18031, which compares the requirements of EN 18031 with ETSI EN 303 645 and EN IEC 62443. These annexes help manufacturers already compliant with these standards understand the extra steps needed for RED DR 2022/30/EU compliance considering that closest standard available for the conformity assessment at the moment that is the EN 18031.
- While ETSI EN 303 645 offers guidance for provisions under EN 18031, it is important to note that ETSI EN 303 645 alone is not enough to meet RED-DA requirements, due to its narrower scope and focus. This requires adjustments in the test cases to fully align with EN 18031.

2. Compliance with the RED-DA outside of the application of harmonised standards:

- The NB reviews the manufacturer's justifications and assesses whether the actions taken demonstrate compliance with the essential requirements of the RED-DA. If insufficient justification is provided, the NB should reject issuing an EU-Type Examination Certificate (TEC).

[13] Standardisation request M/585, European Commission, August 2022.

[14] TIC Council organised a Cybersecurity Hackathons in 2024 in Singapore and Málaga, with the participation of six laboratories. All labs tested according to the ETSI EN 303 645 (V2.1.1). Key takeaways from this exercise included a lack of clarity in some provisions of the standard and challenges related to its interpretation. TIC Council will prepare an in-depth report on the results and aims to engage with standardisation bodies and manufacturers to improve the overall application of the standard.

Contact Person
Ángel Moreno Rubio, Digital Policy Manager
Rue du Commerce 20/22, B-1000 Brussels
Tel: +32 487 02 07 32
Email: amorenorubio@tic-council.org

Editor's Note About TIC Council

TIC Council is the global trade association representing the independent third-party Testing, Inspection and Certification (TIC) industry which brings together about 100-member companies and organizations from around the world to speak with one voice. Its members provide services across a wide range of sectors: consumer products, medical devices, petroleum, mining and metals, food, and agriculture among others. Through provision of these services, TIC Council members assure that not only regulatory requirements are met, but also that reliability, economic value, and sustainability are enhanced. TIC Council's members are present in more than 160 countries and the wider TIC sector currently employs more than 1 million people across the globe.