NIST TEL MRA Program

NB Assessment Checklist

Radio Equipment Directive (2014/53/EU) – RED Articles 3.3 d, e, f (cybersecurity)

Version 1.0 (September 25, 2024)

Introduction

1. By publication of Commission Delegated Regulation (EU) 2022/30[1] as amended by Commission Delegated Regulation (EU) 2023/2444[2], the following three cybersecurity essentials requirements (ERs) for the Radio Equipment Directive (RED) were activated for specific categories and classes of radio equipment.

   RED Article 3.3 d – protection of the network
   RED Article 3.3 e – protection of personal data and privacy
   RED Article 3.3 f – protection from frauds of cybersecurity

2. The date of applicability for RED Articles 3.3 d, 3.3 e, and 3.3 f is **August 1, 2025.**

3. By publication of Implementing Decision C (2022) 5637[3] (M/585) and Amending Implementing Decision C (2023) 5624[4], the European Commission formally provided the standardization request to CEN and CENELEC requesting the drafting of new harmonized standards to support RED Articles 3.3 d, e, f, for the categories and classes of radio equipment specified by Delegated Regulation (EU) 2022/30, with a date of delivery of the first three standards by June 30, 2024.

---

[1] *COMMISSION DELEGATED REGULATION (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive*. [Published in the Official Journal of the European Union (OJEU) on January 12, 2022.]

[2] *COMMISSION DELEGATED REGULATION (EU) 2023/2444 of 20 July 2023 amending Delegated Regulation (EU) 2022/30 as regards the date of application of the essential requirements for radio equipment and correcting that Regulation*

[3] *COMMISSION IMPLEMENTING DECISION of August 5, 2022 on a standardization request to the European Committee for Standardization and the European Committee for Electrotechnical Standardization as regards radio equipment in support of Directive 2014/53/EU of the European Parliament and of the Council and Commission Delegated Regulation (EU) 2022/30.*

[4] *COMMISSION IMPLEMENTING DECISION of August 23, 2023 amending Implementing Decision C (2022) 5637 on a standardization request to the European Committee for Standardization and the European Committee for Electrotechnical Standardization as regards radio equipment in support of Directive 2014/53/EU of the European Parliament and of the Council and Commission Delegated Regulation (EU) 2022/30.*

4. CEN/CENELEC Joint Technical Committee (JTC) 13, Working Group 8 has developed three cybersecurity standards that are available for reference and identified in this checklist. At the time of issuance of this document, the references to these standards are **not cited in the Official Journal of the European Union (OJEU)** and there is no presumption of conformity. RED NB use is currently mandatory for RED Articles 3.3 d/e/f.

5. Scope of radio equipment that must comply with RED Article 3.3 (d) – Protection of the network:

   Any radio equipment that can communicate itself over the internet, whether it communicates directly or via any other equipment

6. Scope of radio equipment that must comply with RED Article 3.3 (e) – Protection of privacy and data:

   Any of the following radio equipment, if that radio equipment is capable of processing, within the meaning of Article 4(2) of Regulation (EU) 2016/679, personal data, as defined in Article 4(1) of Regulation (EU) 2016/679, or traffic data **and** location data, as defined in Article 2, points (b) and (c), of Directive 2002/58/EC:

   (a) internet-connected radio equipment, other than the equipment referred to in points (b), (c) or (d);
   (b) radio equipment designed or intended exclusively for childcare;
   (c) radio equipment covered by Directive 2009/48/EC;
   (d) radio equipment designed or intended, whether exclusively or not exclusively, to be worn on, strapped to, or hung from any of the following:(i) any part of the human body, including the head, neck, trunk, arms, hands, legs and feet; (ii) any clothing, including headwear, hand wear and footwear, which is worn by human beings.

7. Scope of radio equipment that must comply with RED Article 3.3 (f) – protection from fraud

   Any internet-connected radio equipment, if that equipment enables the holder or user to transfer money, monetary value or virtual currency as defined in Article 2, point (d), of Directive (EU) 2019/713.

8. An EU Type Examination Certificate (TEC) for RED Articles 3.3 (d, e, and f) can be issued before the date of applicability of August 1, 2025, but the EU TEC does not become legally applicable until the date of applicability.

9. NIST requires that the RED essential requirements (ERs) for which the NB has been found competent to perform NB activities be listed on the NB's ISO/IEC 17065 Scope of Accreditation. The ERs will be provided to the EC (via NIST NANDO notification) and listed in NANDO (for public viewing). NBs are only able to offer NB services for those essential requirements that are listed in NANDO.

10. This assessment checklist shall be used by the US accreditation bodies to document the technical competency assessment RED NBs that are adding/maintaining RED Articles 3.3 (d, e, and f) on their ISO/IEC 17065 Scope of Accreditation. It is acceptable for the assessment to RED Articles 3.3 (d, e, and f) to be conducted remotely (if the accreditation body allows this).

11. Issues/errors with this document should be reported to the NIST TEL MRA Program (mra@nist.gov).

TO BE COMPLETED BY THE ASSESSOR	
Name of NB	
NB Number	
Accreditation Body Name	
Date(s) of Assessment	
Type of Assessment	___Initial ___Renewal ___Other (Please specify: _____)
Scope of Assessment (Please check all that apply)	____RED Article 3.3 (d) ____RED Article 3.3 (e) ____RED Article 3.3 (f)
Assessor Name	
Assessor Signature	
Accreditation Body Review	AB personnel Name: Date:

Topics and Requirement References	Requirement	NB Document Reference identified by NB	Compliance (Y/N/NA)			Assessor Comments or Additional Assessor Instructions
			d	e	f	
1. Scope of Accreditation						
NIST Requirements & Application for U.S. Conformity Assessment Bodies Seeking EU Radio Equipment Directive (RED) 2014/53/EU Notified Body Status, Section 4	The NB's ISO/IEC 17065 Scope of Accreditation includes reference to one or more of the following essential requirements: RED Articles 3.3 d, e, f					
	For each essential requirement, the NB's ISO/IEC 17065 Scope of Accreditation includes reference applicable categories of radio equipment (within the scope of RED Articles 3.3 d, e, f and the competency of the NB)					
2. EU Scheme Documents						
RED Article 26.6 (b)	The NB has access to Commission Delegated Regulation (CDR) (EU) 2022/30 and has incorporated/referenced this document in the NB's quality management system.					

Topics and Requirement References	Requirement	NB Document Reference identified by NB	Compliance (Y/N/NA)			Assessor Comments or Additional Assessor Instructions
			d	e	f	
	The NB demonstrates an understanding of the scope of CDR (EU) 2022/30					
	The NB can identify the categories of equipment that are applicable RED Articles 3.3 d, e, and f.					
	The NB can identify the categories of equipment that are <u>not</u> applicable for RED Articles 3.3 d, e, and f.					
	The NB has a copy of the latest version of the following CEN/CENELEC standards:	*NIST note to assessors: At the time of issuance of this version of the checklist, the documents have been published but are not cited in the OJEU. See Item 4 in the Introduction.*				
	RED Article 3.3 d - EN 18031-1 (2024)					
	RED Article 3.3 e - EN 18031-2 (2024)					
	RED Article 3.3 f - EN 18031-3 (2024)					

Topics and Requirement References	Requirement	NB Document Reference identified by NB	Compliance (Y/N/NA)			Assessor Comments or Additional Assessor Instructions
			d	e	f	
3. Procedures						
RED Article 26.6 (b)	The NB's certification procedures address the evaluation process for RED Articles 3.3 d, e, f in accordance with the technical and administrative requirements.					
	The NB has developed a cybersecurity checklist to guide the review of the technical documentation or has developed an assessment plan for each application.					
	The NB's client application addresses RED Articles 3.3 d, e, f (as appropriate)					
RED Article 26.11	The NB has access and knowledge of (1) Technical Guidance Notes (TGN), reference documents (REFDOCs), other documents published by the Radio Equipment Directive Compliance Association related to CDR (EU) 2022/30 and cybersecurity.					*NIST note to assessors: TGNs and REFDOCs may not be available yet. The REDCA has posted an RED NB Cyber Checklist Guide (draft V2, 2022) here that NBs should have access to and be familiar with.*

Topics and Requirement References	Requirement	NB Document Reference identified by NB	Compliance (Y/N/NA)			Assessor Comments or Additional Assessor Instructions
			d	e	f	
4. Training Records						
RED Article 26.7 (a)	The NB maintains records of cybersecurity personnel training on **RED Articles 3.3 d, e, f (as appropriate)**					*NIST note to assessors: Please list names of trained cybersecurity personnel here:* Name: Name: Name:
	The NB maintains records of the cybersecurity personnel training **on the NB procedures.**					
5. EU TEC and Associated Evaluation Report						
RED Annex III, Module B, 3 (c) & 4	The NB records demonstrate that the NB is receiving and reviewing the manufacturer's analysis and assessment of risk for RED 3.3 Articles d, e, f (as appropriate)					*NIST note to assessors: For initial assessments, the NB will not have conducted NB activities for RED Articles 3.3 d, e, f yet. In this case, please review and discuss the document referenced in the footnote [5].*

[5] *For initial assessments, the NB shall have available a document describing (a) the minimum elements that the manufacturer must address in their risk assessment with regards to cybersecurity essential requirement, addressing each element at least to the level of granularity of the standardization request [RED Delegated Act (2022/30) Standardization Request (M585) Annex I, Item 2.1, 2.2, and 2.3, and (b) information on the minimally acceptable objective evidence/documentation the NB will accept for each of the elements listed in Annex I, Item 2.1, 2.2, and 2.3. NBs currently provide this document to NIST and the AB as part of the initial cybersecurity assessment readiness check.*

Topics and Requirement References	Requirement	NB Document Reference identified by NB	Compliance (Y/N/NA)			Assessor Comments or Additional Assessor Instructions
			d	e	f	
RED Annex III, Module B, 5	The NB's evaluation report/record documents the objective evidence provided by the applicants to address RED Articles 3.3 d, e, f (as appropriate)					*NIST note to assessors: For initial assessments it is sufficient to verify that this is stated in the procedures and document noted in footnote 5 since the NB has not yet conducted NB activities for RED Articles 3.3 d, e, f*
RED Annex III, Module B, 6	The NB's EU Type Examination Certificate correctly addresses RED Articles 3.3 d, e, f (as appropriate)					*NIST note to assessors: For initial assessments it is sufficient to verify that this is demonstrated in a draft EU TEC since the NB has not yet conducted NB activities for RED Articles 3.3 d, e, f*
EG RE (06) Q&A, Item 21, last paragraph	The NB is aware of the EC's interpretation that (a) the RED essential requirements are considered separate "aspects", (b) that a manufacturer may use a different NB for each "aspect" or essential requirement and (c) may identify more than one RED NB on its Declaration of Conformity (DoC)					

Topics and Requirement References	Requirement	NB Document Reference identified by NB	Compliance (Y/N/NA)			Assessor Comments or Additional Assessor Instructions
			d	e	f	
6. Technical Competency						
General Cybersecurity Knowledge	**The NB demonstrates an understanding of the following cybersecurity topics/areas of knowledge:**					
	Cybersecurity risks, threats, and vulnerabilities					
	Cybersecurity attack vectors, tactics, and vulnerabilities					
	Penetration testing tools, techniques, and methodologies					
	Threat taxonomies and vulnerability repositories					
	TTP (Tactics, Techniques, and Procedures) frameworks					
	Secure development lifecycle (SDLC) and security-by-design concepts					
	Privacy-by-design methodologies					
	Privacy-Enhancing Technologies (PETs)					

Topics and Requirement References	Requirement	NB Document Reference identified by NB	Compliance (Y/N/NA)			Assessor Comments or Additional Assessor Instructions
			d	e	f	
RED Articles 3.3 d/e/f *Implementing Decision C (2022) 5637 (M/585) – See Note 1.* and *EN 18031-1 (2024)* *EN 18031-2 (2024)* *EN 18031-3 (2024)* *Note: The applicable elements noted in this checklist are based on each standard's ZA Annex list of relevant normative clauses identified by the authors as those deemed to minimally be required to demonstrate compliance with the essential requirements. However, please note that as of 9/17/2024, the references to these 3 EN standards are not cited in the OJEU.*	**The NB demonstrates:** **(1) an understanding of the technical requirements listed in Implementing Decision C (2022) 5637 (M/585) and how the (a) mechanisms, (b) security requirements, and (c) assessment criteria included in the EN 10831-1, -2, and -3 series correlate to those technical requirements. See Note 1 on page 15 of this document.** **(2) the ability to correctly check for and evaluate the manufacturer's technical documentation, including the risk assessment, to determine whether the technical requirements (M/585) are correctly addressed by the manufacturer if applicable** **(3) the ability to correctly determine whether compliance with RED Articles 3.3 d, e, and/or f has been demonstrated at the level of the technical requirements listed in Implementing Decision C (2022) 5637[6] (M/585), as further defined through the mechanisms identified in the referenced EN standards where relevant, whether the manufacturer is using these referenced EN standards or other standards:**					
			d	e	f	
	Access control mechanism - ACM					
	Authentication mechanism – AUM					
	Secure update mechanism - SUM					
	Secure storage mechanism - SSM					

[6] *COMMISSION IMPLEMENTING DECISION of August 5, 2022 on a standardization request to the European Committee for Standardization and the European Committee for Electrotechnical Standardization as regards radio equipment in support of Directive 2014/53/EU of the European Parliament and of the Council and Commission Delegated Regulation (EU) 2022/30.*

Topics and Requirement References	Requirement	NB Document Reference identified by NB	Compliance (Y/N/NA)			Assessor Comments or Additional Assessor Instructions
			d	e	f	
	Secure communication mechanism - SCM					
	Resilience mechanism - RLM					
	Network monitoring mechanism - NMM					
	Traffic control mechanism – TCM					
	Confidential cryptographic keys (CCK)					
	Logging mechanism - LGM					
	Deletion mechanism - DLM					
	User notification mechanism - UNM					
	General equipment capabilities (GEC):	*Clause 6.10*				
	Up-to-date software and hardware with no publicly known exploitable vulnerabilities					
	Limit exposure of services via related network interfaces					

Topics and Requirement References	Requirement	NB Document Reference identified by NB	Compliance (Y/N/NA)			Assessor Comments or Additional Assessor Instructions
			d	e	f	
	Configuration of optional services and related exposed network interfaces					
	Documentation of exposed network interfaces and exposed services via network interfaces.					*Informative only*
	No unnecessary external interfaces					
	Input validation					
	Documentation of external sensing capabilities					*Informative only*
	Equipment integrity					
	Cryptography – CRY					
Legal Requirements EN 18031-1 (2024) EN 18031-2 (2024) EN 18031-3 (2024)	The NB has procedures for how to address situations where there are additional legal requirements that may conflict with the referenced cybersecurity standards.					*Specific known issue at the time of publication of this version of the checklist that conflicts with the access control mechanism requirements: Measuring Instruments Directive (MID: 2013/32/EU) Annex I, 10.5 requires that a display needs to be able to display index values (which is considered as personal data) and this must be accessible without tools to the consumer.*

Topics and Requirement References	Requirement	NB Document Reference identified by NB	Compliance (Y/N/NA)			Assessor Comments or Additional Assessor Instructions
			d	e	f	
7. **Relevant cybersecurity standards and other resources**						
	The NB has access to and is knowledgeable about the requirements and information in the following standards/publications:					
	ETSI EN 303 645 - CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements					
	ETSI TS 103 701: CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements					
	IEC 62443-4-2 - Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components					
	ETSI TS 103 929: Mapping of specific requirements of standardization request for RED articles 3(3)(d), 3(3)(e) and 3(3)(f) to IEC 62443-4-2 requirements and to ETSI EN 303 645 provisions					

Topics and Requirement References	Requirement	NB Document Reference identified by NB	Compliance (Y/N/NA)			Assessor Comments or Additional Assessor Instructions
			d	e	f	
	ISO/IEC 27402 (Cybersecurity – IoT security and privacy – Device baseline requirements)					
	ANSI/CTA-2088-A - Baseline Cybersecurity Standard for Devices and Device Systems					
	NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline					
	Technical Competency Requirements for Accreditation of Conformity Assessment Bodies for the purposes of notification according to the RED Directive SCOPE: Article 3.3 d, e, f (Draft, 7/2022, V1, Spain)					See www.redca.eu documents.
	Other					Identify here or attach a list.

NOTES

Note 1: Excerpt from Implementing Decision C (2022) 5637[7] (M/585)

2. Requirements for specific standards

2.1. Harmonised standards in support of the essential requirement set out in ***Article 3(3), point (d),*** *of Directive 2014/53/EU for the categories and classes specified by Delegated Regulation (EU) 2022/30 shall contain technical specifications that ensure at least that those radio equipment, where applicable:*

(a) include elements to monitor and control network traffic, including the transmission of outgoing data;

(b) are designed to mitigate the effects of ongoing denial of service attacks;

(c) implement appropriate authentication and access control mechanisms;

(d) are provided, on a risk basis, with up-to-date software and hardware at the moment of placing on the market that do not contain publicly known exploitable vulnerabilities as regards harm to the network or its functioning or misuse of network resources;

(e) are provided with automated and secure mechanisms for updating software or firmware that allow, when necessary, the mitigation of vulnerabilities that if exploited may lead to the radio equipment harming the network or its functioning or the misuse of network resources;

(f) protect the exposed attack surfaces and minimise the impact of successful attacks.

2.2. Harmonised standards in support of the essential requirement set out in ***Article 3(3), point (e),*** *of Directive 2014/53/EU for the categories and classes specified by Delegated Regulation (EU) 2022/30 shall contain technical specifications that ensure at least that those radio equipment, where applicable:*

[7] *COMMISSION IMPLEMENTING DECISION of August 5, 2022 on a standardization request to the European Committee for Standardization and the European Committee for Electrotechnical Standardization as regards radio equipment in support of Directive 2014/53/EU of the European Parliament and of the Council and Commission Delegated Regulation (EU) 2022/30.*

(a) protect stored, transmitted or otherwise processed personal data against accidental or unauthorised processing, including storage, access, disclosure, destruction, loss or alteration or lack of availability;
(b) implement appropriate authentication and access control mechanisms;
(c) are provided, on a risk basis, with up-to-date software and hardware at the moment of placing on the market that do not contain publicly known exploitable vulnerabilities as regards data protection and privacy;
(d) are provided with automated and secure mechanisms for updating software or firmware that allow, when necessary, the mitigation of vulnerabilities that if exploited may lead to unauthorised processing, including storage, access, disclosure, destruction, loss or alteration or lack of availability of personal data;
(e) include functionalities to inform the user of changes that may affect data protection and privacy;
(f) log the internal activity that can have an impact on data protection and privacy;
(g) allow users to easily delete their stored personal data, enabling the disposal or replacement of equipment without the risk of exposing personal data;
(h) protect the exposed attack surfaces and minimise the impact of successful attacks.

2.3. Harmonised standards in support of the essential requirement set out in ***Article 3(3), point (f),*** *of Directive 2014/53/EU for the categories and classes specified by Delegated Regulation (EU) 2022/30 shall describe technical specifications that ensure at least that those radio equipment, where applicable:*
(a) protect stored, transmitted or otherwise processed financial or monetary data against accidental or unauthorised processing, including storage, access, disclosure, destruction, loss or alteration or lack of availability;
(b) implement appropriate authentication and access control mechanisms;
(c) are provided, on a risk basis, with up-to-date software and hardware at the moment of placing on the market that do not contain publicly known exploitable vulnerabilities as regards financial or monetary data;

(d) are provided with automated and secure mechanisms for updating software or firmware that allow, when necessary, the mitigation of vulnerabilities that if exploited may lead to unauthorised processing, including storage, access, disclosure, destruction, loss or alteration or lack of availability of financial or monetary data;

(e) log the internal activity that can have an impact on financial or monetary data;

(f) protect the exposed attack surfaces and minimise the impact of successful attacks.

Note 2: Source Information

*Some of the elements of this checklist come from the Ministerio de Asuntos Economicos y Transformacion Digital - TECHNICAL COMPETENCY REQUIREMENTS **ASSESSMENT GUIDE** for Accreditation of Conformity Assessment Bodies for the purposes of Notification according to the RED Directive [SCOPE: Article 3.3 d, e, f] – Draft 6/2022, V2 - Spain).*

DOCUMENT CONTROL

Action	**Date**	**Comments**
Initial Release	September 25, 2024	