Annex – Standard: ISO/IEC27001 and extension to the guidelines ISO/IEC27xxx

Edition: March 2023

CHAPTER 1 - GENERAL

These Rules define the additional and/or substitutive procedures applied by RINA for the certification of Qualitty Management Systems in relation to what is already defined in the Document *General Rules for the Certification of Management Systems RC/40*

RINA issues certification in accordance with the requirements of the ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015/Amd.1:2020 Rules to organizations whose Management System has been recognized as fully conforming to all the requirements of the Standard:

ISO/IEC 27001:2022

and until 29th april 2024, as an alternative, for the standard:

ISO/IEC 27001:2013 (UNI CEI EN ISO/IEC 27001:2017)

The certification may be extended to the guidelines:

ISO/IEC 27017: 2015
ISO/IEC 27018: 2019
ISO/IEC 27701: 2019
ISO/IEC 27035-1:2016, ISO/IEC 27035-2:2016, ISO/IEC27035-3:2020

From 30 April 2024, all new certifications and recertifications must be issued exclusively in conformity with ISO/IEC 27001:2022.

CHAPTER 2 - REFERENCE STANDARD / CERTIFICATION REQUIREMENTS

In addition to what is stated in the General Rules for the Certification of Management Systems, to obtain RINA certification, a Quality Management System must first and henceforth be compliant to the requirements of ISO/IEC 27001 and the additional requirements of Accreditation Bodies (e.g. Accredia technical document no. 02/2018…).

The extension to the guidelines must take place with a valid ISO/IEC 27001 certification, accredited by an Accreditation Body signatory of the mutual recognition agreement IAF/MLA (IAF – International Accreditation Forum/MLA - Multilateral Agreements). The ISO/IEC 27001 certification scope must be compatible with the guidelines processes to be integrated with.

If the organization has been granted an ISO/IEC 27001 certification issued by another Certification Body with MLA accreditation, the organization must request the transfer of certification to RINA before extension to the Guidelines as described in Chapter 10 of the General Regulation for the certification of Management Systems.

If the organization has not been granted an ISO/IEC 27001 certification issued by another Certification Body with MLA accreditation, the organization must request a new certification from RINA.

The extension of certification to ISO/IEC 27017:2015 alone is allowed, while the extension to ISO/IEC 27018:2019 must always be preceded by an extension to ISO/IEC 27017:2015. Contextual extension to ISO/IEC 27017:2015 and ISO/IEC 27018:2019 guidelines is allowed.

The extension of the certification to the ISO/IEC 27701:2019 and ISO/IEC 27035 part 1, 2 and 3 guidelines individually is allowed.

CHAPTER 3 – FIRST CERTIFICATION

The documents *General Rules for the Certification of Management Systems RC/40* and the provisions of the "*General contract conditions for the certification of systems, products and personnel*" are applicable.

In addition, the following applies.

Organizations wishing to obtain certification of their Information Security Management System and/or extension to the guidelines must send RINA in addition to the Application Form also the specific ATTACHMENT TO THE APPLICATION FOR ISO/IEC 27001 (ISMS) and ISO/IEC 27XXX:20YY, available on the www.rina.org website, filled in in all its parts.

In particular, the Application Form gathers information on:

- Datacenters where the servers that manage the service / sites where critical assets are located are located;
- Factors related to the activity carried out and the organization;
- IT environmental factors;
- Factors that could lead to reductions or increases in the duration of audit time.

This information must be sent by an authorized representative of the applying organization.

If the Information Security Management System includes documentation (procedures, records, etc.) classified as "confidential" and/or otherwise not available for certification purposes. RINA will assess the existence of the conditions to be able to continue the certification process.

The audit for the extension to the guidelines must be carried out entirely at the site or sites of the Organization including the data centers where the ICT infrastructure is located. If the type of ICT infrastructure does not allow to carry out an on-site audit (e.g. suppliers such as AWS, AZURE), the contractual agreements between the Organization and the suppliers and the operational control aspects implemented must be verified.

Certification documents may refer to national and international standards as a source(s) of controls for those that are considered necessary in the organization's Statement of Applicability. The reference on the certification documents must be point to the source(s) of controls applied in the Statement of Applicability and not as a certification against the standards themselves.

CHAPTER 4 - MAINTAINING VALIDITY OF THE CERTIFICATE

The documents *General Rules for the Certification of Management Systems RC/40* and the provisions of the "*General contract conditions for the certification of systems, products and personnel*" are applicable.

CHAPTER 5 - RECERTIFICATION

The documents *General Rules for the Certification of Management Systems RC/40* and the provisions of the "*General contract conditions for the certification of systems, products and personnel*" are applicable.

In addition, the following applies.

On the Management System recertification audit, scheduled every three years, the Organization must send RINA in addition to the Application Form also the specific **ATTACHMENT TO THE APPLICATION FORM ISO/IEC 27001 (ISMS) and ISO/IEC 27XXX:20YY offer**, available on the www.rina.org website, completed in all its parts as described in point 3 of this regulation.

CAPITOLO 6 – AUDIT CONDUCTION

The documents *General Rules for the Certification of Management Systems RC/40* and the provisions of the "*General contract conditions for the certification of systems, products and personnel*" are applicable

In addition, the following applies:

The audit for the extension to the guidelines must be carried out entirely at the site or sites of the Organization including the data centers where the ICT infrastructure is located as described in point 3 of this regulation.

The on-site audit time must not be less than 70% of the total audit time.

CAPITOLO 7 - MANAGEMENT OF CERTIFICATES OF CONFORMITY

The documents *General Rules for the Certification of Management Systems RC/40* and the provisions of the "*General contract conditions for the certification of systems, products and personnel*" are applicable

CAPITOLO 8 - MODIFICATION OF CERTIFICATION AND COMMUNICATION OF CHANGES

The documents *General Rules for the Certification of Management Systems RC/40* and the provisions of the "*General contract conditions for the certification of systems, products and personnel*" are applicable

CAPITOLO 9 - SPECIAL REQUIREMENTS FOR MULTI-SITE ORGANISATIONS

The documents *General Rules for the Certification of Management Systems RC/40* and the provisions of the "*General contract conditions for the certification of systems, products and personnel*" are applicable

In addition, the following applies.

The sampling of the sites to be audited may also include the data centers where the ICT infrastructure is located. RINA assesses the applicability of sampling in addition to the criteria defined in the General Regulation for the certification of Management Systems also:

- the results of internal headquarters and site audits or previous certification audits;

- complexity of the Management System;
- complexity of the IT systems of the different sites;
- potential interaction with critical IT systems or IT systems handling sensitive data;
- risk assessment.

The central function of the Organization must also participate in the definition and management of the security policy, risk assessment, analysis and treatment, definition, management and analysis of controls, definition and management of the Statement of Applicability.

CAPITOLO 10 - TRANSFER OF ACCREDITED CERTIFICATES

The documents *General Rules for the Certification of Management Systems RC/40* and the provisions of the "*General contract conditions for the certification of systems, products and personnel*" are applicable

In addition, the following applies.

If an Organization with valid a certification issued by another Management Systems Certification Body, accredited by an Accreditation Body that adheres to the IAF/MLA mutual recognition agreement, wants to transfer its certification to RINA, it must send to RINA in addition to the Application Form also the specific **ANNEX TO THE APPLICATION FORM FOR ISO/IEC 27001 (ISMS) and ISO/IEC 27XXX:20YY**. , available on the www.rina.org website, completed in all its parts, as described in point 3.1 of this regulation, copy of the Management System certificate and copy of the Statement of Applicability whose reference is shown on the certificate.

CAPITOLO 11 - SUSPENSION, REINSTATEMENT AND WITHDRAWAL OF CERTIFICATION

The documents *General Rules for the Certification of Management Systems RC/40* and the provisions of the "*General contract conditions for the certification of systems, products and personnel*" are applicable

CAPITOLO 12 - RENUNCIATION OF CERTIFICATION

The documents *General Rules for the Certification of Management Systems RC/40* and the provisions of the "*General contract conditions for the certification of systems, products and personnel*" are applicable

CAPITOLO 13 - CONTRACTUAL CONDITIONS

The documents *General Rules for the Certification of Management Systems RC/40* and the provisions of the "*General contract conditions for the certification of systems, products and personnel*" are applicable

SPECIFIC RULES FOR THE TRANSITION OF CERTIFICATION FROM ISO/IEC 27001: 2013 (UNI CEI EN ISO/IEC 27001:2017) TO ISO/IEC 27001: 2022

A.1 – TRANSITION REQUEST

During the transition period, the Organization already certified to the ISO/IEC 27001: 2013 (UNI CEI EN ISO/IEC 27001:2017) standard can choose to make the transition to the new standard:

1. in conjunction with a surveillance audit with a minimum increase of 1.0 auditor day
2. in conjunction with a recertification audit with a minimum increase of 0.5 auditor day
3. between two scheduled audits with a minimum effort of 1.0 auditor day

The request to carry out the transition must be requested to RINA by an authorized representative of the requesting organization.

A.2 – TRANSITION AUDIT EXECUTION

The transition audit consists of an on-site audit to verify the application of the new conformity requirements of ISO/IEC 27001: 2022.

For what regards the methods of conducting the audit, see the provisions of the General Regulation for the certification of Management Systems.

The transition audit will include the following elements:

- the gap analysis of ISO/IEC 27001:2022, as well as the need for changes to the Information Security Management System;
- exam of the updated Statement of Applicability (SoA);
- where applicable, exam of the updated risk treatment plan;
- exam of the implementation and effectiveness of new or modified controls chosen by the organization;

During the transition period, if major non-conformities with respect to the ISO/IEC 27001:2022 are found and not corrected within the deadlines defined in the General Regulation for the certification of Management Systems, such non-conformities will not adversely affect the maintenance of valid certification, provided, of course, that it is verified that the information security management quality management system continues to maintain compliance with ISO/IEC 27001: 2022.

The periodicity and extent of subsequent audits for the maintenance of the certification are unchanged and follow the provisions of the three-year audit program.

A.3 – CONFORMITY CERTIFICATES WITH INTEGRATION TO GUIDELINES ISO/IEC 27XXX:20YY SPECIAL FEATURES

The transition audit, for organizations already certified ISO/IEC 27001: 2013 (UNI CEI EN ISO/IEC 27001: 2017) with integration to the guidelines listed in point 1.2 of this regulation, in addition to what is defined in point A.2 of this regulation, will include a verification of the Statement of Applicability (SoA) with regard to the specific controls defined in the guidelines, new or modified chosen by the organization.

A.4 – ISO/IEC 27001: 2022 CONFORMITY CERTIFICATE ISSUING

Upon successful completion of the transition audit and after validation by RINA, a Certificate of Conformity to the new edition of the standard is issued, the validity of which will be calculated based on the previous decision date for certification/recertification.

A.5 – VALIDITY OF ISO/IEC 27001: 2013 (UNI CEI EN ISO/IEC 27001: 2017) CONFORMITY CERTIFICATES

The certifications of conformity to the requirements of the certified standard ISO/IEC 27001: 2013 (UNI CEI EN ISO/IEC 27001: 2017) will expire on October 31st, 2025.

The Organization that, after the expiry date of the certificate, intends to access the certification again, must submit a new application following the entire procedure provided for the initial certification.