Supplementary Appendix – Certification Standard: ISO 37301

Edition: April 2025

CHAPTER 1 – GENERAL

This Appendix defines the additional and/or replacement procedures applied by RINA for the certification of Compliance Management Systems, with respect to what is already defined in the General Regulation for the Certification of RC/C Management Systems 40.

RINA issues certification in accordance with the requirements of the ISO/IEC 17021-1:2015 standard to Organizations whose Management System has been recognized as compliant with all the requirements of the standard:

ISO 37301:2021

In addition to the provisions of the General Regulation for the Certification of RC/C 40 Management Systems, in order to obtain certification by RINA, an Anti-Corruption Management System must initially and over time meet the requirements of the ISO 37301:2021 standard and the additional requirements provided by the Accreditation Bodies for the ISO 37301 scheme.

CHAPTER 2 - REFERENCE STANDARD / REQUIREMENTS FOR CERTIFICATION

The ISO 37301:2021 certification is issued to a legal entity in its entirety, and to all its departments/subsidiaries, processes and activities actually carried out.

It must be clarified in the scope of application whether the organization holds control over other organizations, specifying the characteristics of such control (e.g. equity participations, contractual constraints, etc.), in case these fall within the scope of the certificate.

It is not allowed to limit the application of the CMS to certain processes or functions, or to specific sites of the organization or controlled organizations.

It is permissible that in the first instance the scope of certification is limited to the business processes involved in the management of the most relevant compliance risks. These risks and processes must be identified by the organization through the "compliance risk assessment".

In the event that the organization requests, on the basis of the compliance risk assessment, to undertake a progressive certification process, it must present the program for extending the scope of certification to business processes in order to achieve complete coverage of the compliance areas.

However, as part of the identified process(s), the organization must mandatorily include "all" compliance areas (e.g. privacy and data protection, safety, anti-money laundering, administrative liability, security and others) pertaining to that process

In order to be fully operational, the Compliance Management System, in addition to the provisions of the General Regulation for the Certification of Management Systems, must ensure that:

- The size, structure and decision-making authority of the organization has been determined
- The places and sectors in which the organization operates have been determined
- The nature, size and complexity of the organisation's activities and operations have been determined;
- The organization's business model has been determined;
- The relevant stakeholders for the compliance management system and their requirements have been determined
- The subjects over whom the organization has control and the entities that exercise control over the organization have been determined;

- Have been determined business partners of the organization;
- A mapping of compliance obligations has been carried out, which include mandatory requirements, which an organisation must comply with, but also voluntary requirements, which an organisation chooses to comply with.
- Compliance risk assessment has been carried out on all processes and activities
- Roles, responsibilities and authorities have been identified for the management of compliance, with specific requirements and assignment of tasks and powers necessary to supervise and ensure compliance of the system and report to top management on the effective implementation and effectiveness of the system itself;
- A Compliance Policy has been adopted, which can also encourage the reporting of suspected violations and retaliation

The Organization must have a document in which the purpose is determined, considering the provisions of the requirements 4.1, 4.2, 4.3, 4.4 and 4.5 of the ISO 37301:2021 standard and the documented information as required by point 7.5 of the reference standard.

In establishing the audit program, the size of the organization, the scope of application and the complexity of the Management System are taken into account. For the purpose of determining the complexity class, the products and processes provided, the level of effectiveness of the Management System, the result of previous audits or other audits already carried out, as well as internal and external factors such as judicial investigations, accidents, multinational transactions, complex governance, company size, sector of activity and regulatory requirements are considered.

CHAPTER 3 - INITIAL CERTIFICATION

In addition to the provisions of the General Regulation for the Certification of RC/C Management Systems 40, in addition to the provisions of point 3.1 of the General Regulation for the certification of management systems, the organization must provide RINA with information regarding:

- Compliance obligations applicable to the organization with reference to mandatory legislation, voluntary rules (ISO, guidelines, best practices), critical contractual provisions/clauses, sector regulatory rules;
- the assessment of compliance obligations to which the most significant risks for all processes/activities are associated;
- the "compliance risk assessment" document defined by the organization in accordance with the requirements of the ISO 37301 standard at § 4.6;
- the perimeter within which the Compliance Management System is applied, indicating the processes, sites and offices involved;
- the program to extend the certification to all processes, sites and company offices involved (where applicable);
- context analysis;
- mapping processes (internal and external) and listing the relevant applicable laws, rules and rules;
- corporate relations with third parties and specific legislative references;
- the indication of third-party companies and their compliance, as well as management methods;
- the analysis of episodes or threats of violation of compliance and the countermeasures adopted;
- the records concerning the methods of managing court cases and measures in which the organization is involved and, where applicable, the evidence of the involvement and intervention of the Supervisory Body.

With reference to the documentation that the Organization must make available to RINA, the availability of the Organization's management manual and the list of internal procedures is not mandatory. The above documentation is assessed by RINA for compliance with the reference standard and the requirements of these Rules.

CHAPTER 4 - MAINTENANCE OF CERTIFICATION

The provisions of the Rules for the certification of RC/C management systems 40 apply

CHAPTER 5 - RECERTIFICATION

The provisions of the Rules for the certification of RC/C management systems 40 apply

CHAPTER 6 - AUDIT PERFORMANCE

The provisions of the Rules for the certification of RC/C management systems 40 apply

CHAPTER 7 - MANAGEMENT OF CERTIFICATES OF CONFORMITY

The provisions of the Rules for the certification of RC/C management systems 40 apply

CHAPTER 8 - MODIFICATION OF CERTIFICATION AND COMMUNICATION OF CHANGES

The provisions of the Rules for the certification of RC/C management systems 40 and the provisions of the "GENERAL TERMS AND CONDITIONS FOR THE CERTIFICATION OF SYSTEMS, PRODUCTS AND PERSONNEL" apply.

In addition to the provisions of the Regulation for the certification of RC/C management systems 40 and the provisions of the "GENERAL TERMS AND CONDITIONS OF CONTRACT FOR THE CERTIFICATION OF SYSTEMS, PRODUCTS AND PERSONNEL", an organization certified or in the process of certification must promptly inform and keep RINA updated when it is involved in any critical situation that could compromise the guarantee of the certification of the system (e.g. news of public interest that damage the reputation of the company, or involvement in legal proceedings for breach of compliance).

In the same way, the organization must promptly notify RINA of any ongoing legal proceedings, and of the consequent actions taken to contain the effects of such event, therefore of the analysis of the root causes and the related corrective actions.

The information is also due if the events should involve top figures for other areas or non-certified sites/processes.

RINA, in response to these reports, coming directly from the organization or from other sources, will carry out the necessary specific investigations and investigations and may adopt the appropriate measures including: filing of the report, sanctions, strengthening of the inspection activity, defined according to the adequacy of the response and strategies adopted by the organization.

CHAPTER 9 - PARTICULARITIES FOR MULTI-SITE ORGANIZATIONS

In addition to the provisions of the General Regulation for the certification of RC/C Management Systems 40, where significant risks are managed at a site of the organization in the light of the assessment of compliance risks, the governance of these risks must be assessed during the initial certification and in subsequent surveillance on the basis of the sampling identified in the three-year plan.

CHAPTER 10 - TRANSFER OF ACCREDITED CERTIFICATES

The provisions of the Rules for the certification of RC/C management systems 40 apply

CHAPTER 11 - SUSPENSION, REINSTATEMENT AND REVOCATION OF CERTIFICATION

The provisions of the Rules for the certification of RC/C management systems 40 and the provisions of the "GENERAL TERMS AND CONDITIONS FOR THE CERTIFICATION OF SYSTEMS, PRODUCTS AND PERSONNEL" apply.

CHAPTER 12 - WAIVER OF CERTIFICATION

The provisions of the Rules for the certification of RC/C management systems 40 apply

CHAPTER 13 - CONTRACTUAL CONDITIONS

The provisions of the Rules for the certification of RC/C management systems 40 and the provisions of the "GENERAL TERMS AND CONDITIONS FOR THE CERTIFICATION OF SYSTEMS, PRODUCTS AND PERSONNEL" apply.