# Information Security Management Systems Certification Regulation and guidelines ISO/IEC 27xxx extension

*Valid from 15th March 2023*

RINA
Via Corsica 12
I-16128 Genoa - Italy

Phone # +39 010 53851 Fax #
+39 010 5351000 website
www.rina.org

---

Technical regulations

This regulation is divided into three sections:

Section 1:

Certification of Information Security Management Systems in conformity with ISO/IEC 27001: 2022

Section 2:

Certification of Information Security Management Systems in conformity with ISO/IEC 27001: 2013 (UNI CEI EN ISO/IEC 27001:2017)

Section 3:

Transition of certification from ISO/IEC 27001: 2013 (UNI CEI EN ISO/IEC 27001:2017) to ISO/IEC 27001: 2022

**TABLE OF CONTENT**

# SECTION 1: CERTIFICATION OF INFORMATION SECURITY MANAGEMENT SYSTEMS IN CONFORMITY WITH TO ISO/IEC 27001: 2022

## CHAPTER 1 INTRODUCTION

**1.1**

This regulation defines the additional and/or different procedures applied by RINA for the certification of Information Security Management Systems with respect to what has already been defined in:

**General Regulation for the certification of Management Systems**.

The points of this regulations refer to and maintain the same numbering of the corresponding points of the General Regulations for the Certification of Management Systems for which amendments and/or additions have been made.

**1.2**

RINA issues the certification in conformity with the requirements of ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015 to organizations whose Information Security Management System has been recognized as complying with all the requirements of the standard:

**ISO/IEC 27001: 2022**

The certification can be integrated with 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**

The extension to the guidelines must take place together with a valid ISO/IEC 27001:2022 certification, accredited by an Accreditation Body that adheres to the mutual recognition agreement IAF/MLA (IAF – International Accreditation Forum/MLA - Multilateral Agreements). The scope of ISO/IEC 27001:2022 certification must be compatible with the processes of the Guidelines whose integration is requested.

If the organization has not been granted an ISO/IEC 27001:2022 certificate issued by another Certification Body with MLA accreditation, the organization must require the transfer of the certification to RINA before extending it 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 27001:2022 certificate issued by another Certification Body with MLA accreditation, the organization must request a new certification from RINA.

The extension of the 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.

Extension of certification to ISO/IEC 27701:2019 alone is allowed.

## CHAPTER 3 FIRST CERTIFICATION

**3.1**

Organizations that would like to be granted a 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 **ANNEX TO THE APPLICATION FORM FOR ISO/IEC 27001 (ISMS) and ISO/IEC 27XXX:20YY quotation**, available at the www.rina.org website, filled in in all its parts.

In particular, the Application Form requires that information be provided 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;
- Factors related to the IT environment;
- Factors that could lead to reductions or increases in the duration of audit time.

The information must be received from an authorized representative of the requesting 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.

**3.5**

The audit for the extension to the guidelines must be conducted 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 conduct 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.

**3.6**

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 indicative of the source(s) of controls applied in the Declaration of Applicability and not as a certification against the standards themselves.

## CHAPTER 5 RECERTIFICATION

**5.1**

At the time of the Management System recertification audit, scheduled every three years, the organization must send RINA the application form and the specific ANNEX TO THE APPLICATION FORM FOR THE ISO/IEC 27001 (ISMS) and ISO/IEC 27XXX:20YY, available on the RINA web site www.rina.org. The two documents must be duly filled in as described in paragraph 3.1 of this regulation.

## CHAPTER 6 CONDUCTING THE AUDIT

### 6.1 INTRODUCTION

**6.1.1**

The guidelines extension audit must be completely carried out at the organization's site(s), including the datacenter(s) hosting the ICT infrastructure, as described in paragraph 3.5 of this regulation.

On-site audit time must be at least 70% of the total audit time.

The audit for organizations with guidelines integration will include a verification of the Statement of Applicability (SoA) regarding the specific controls defined in the guidelines, new or modified chosen by the organization.

## CHAPTER 9 MULTISITE ORGANIZATIONS SPECIAL FEATURES

**9.1**

Site sampling to conduct the audit may also include the datacenter(s) hosting the organization's ICT infrastructure. RINA will evaluate the applicability of the sampling process according to the General Regulation for the Management Systems Certification and according to the following elements:

- the central function and site(s) internal audits results or the audit results of past certification audits;
- the Management System complexity;
- the site(s)'s IT system complexity;
- potential interactions with critical IT system(s) or with sites managing sensitive data;
- the risk evaluation;

The organization's central function must partake to the security policy definition and management, to the risk evaluation, the analysis and processing, definition, management and analysis of the controls, definition and management of the Statement of Applicability.

## CHAPTER 10 ACCREDITED CERTIFICATES TRANSFER

**10.1**

If an organization with a valid certification issued by another management systems certification body that is accredited by an accreditation organization signatory of the IAF/MLA would like to transfer its own certification to RINA, the organization must send RINA the application form and the specific ANNEX TO THE APPLICATION FORM FOR THE ISO/IEC 27001 (ISMS) AND ISO/IEC 27XXX:20YY, that is available on the RINA web site www.rina.org. The documents must be duly filled in as described in paragraph 3.1 of this regulation, together with a copy of the Management System certificate, and a copy of the Statement of Applicability whose references are also included on the certificate itself.

# SECTION 2: CERTIFICATION OF INFORMATION SECURITY MANAGEMENT SYSTEMS IN CONFORMITY WITH ISO/IEC 27001: 2013 (UNI CEI EN ISO/IEC 27001:2017)

## CHAPTER 1 INTRODUCTION

**1.1**

This regulation describes the procedures that RINA applies to certify the Information Security Business Management Systems in addition to or as an alternative to the ones defined in:

**Management Systems Certification General Regulation**.

This document details which points of the Management System Certification General Regulation are superseded by this regulation. The paragraph numbering is the same as the Management Systems Certification General Regulation to make is easier examining it together with this regulation.

**1.2**

RINA issues the certification in conformity with to the requirements ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015 only for organization whose Management System has been declared compliant to every requirement of:

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

The certification can be integrated with the following 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**

The extension to the guidelines can be applied only on a valid certification ISO/IEC 27001:2013 (UNI CEI EN ISO/IEC 27001:2017), that is accredited by an Accreditation Organization that is a signatory of IAF – International Accreditation Forum/MLA - Multilateral Agreements. The ISO/IEC 27001:2013 certification scope must be compatible with the guidelines processes for which the integrability has been asked.

If the organization has already obtained the ISO/IEC 27001:2013 certification from another MLA accredited certification body, it must ask RINA to transfer the certification to RINA before proceeding with the extension to the guideline, as described in chapter 10 of the Management System Certification General Regulation.

If the organization does not already have the ISO/IEC 27001:2013 certification issued by another MLA accredited certification body, it must ask RINA for a new certification.

It is possible to extend the certification to the ISO/IEC 27017:2015 guideline alone, while the extension to the ISO/IEC 27018:2019 guideline must always be preceded by the extension to the ISO/IEC 27017:2015 guideline. It is possible to extend at the same time both the ISO/IEC 27017:2015 and the ISO/IEC 27018:2019.

It is possible to extend the certification to the ISO/IEC 27701:2019 alone.

**1.3**

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

## CHAPTER 3 FIRST CERTIFICATION

**3.1**

The organization that would like to certify their Information Security Management System and/or obtain the extension to the guidelines must send RINA the application form and the specific **ANNEX TO THE APPLICATION FORM FOR ISO/IEC 27001 (ISMS) QUOTATION,** that is available on the RINA website www.rina.org. Both the application form and the annex must be duly filled in.

To complete the application form, the following information is required:

- Datacenters where the servers managing the service are deployed / the sites hosting critical assets;
- Factors concerning the organization and its business;
- Factors concerning the IT environment;
- Factors that might increase or decrease the audit time.

The above-listed information must be obtained from an organization's legal representative.

If the ISMS includes documentation (procedures, records, etc.) that is confidential and, in any case, not available for the certification process, RINA will evaluate on a case-by-case basis whether it is possible to carry on the certification process.

**3.5**

The guidelines extension audit must be executed completely at the organization's site(s), including the datacenter(s) hosting the ICT infrastructure. In case the ICT infrastructure type does not allow for an on-site audit (e.g., suppliers as AWS, AZURE), the agreements between the organization and the supplier(s) will have to be examined and the operational controls in place.

**3.6**

The certification documents may reference national and international standards as source(s) of control set for controls that are determined as necessary in the organization's Statement of Applicability. The reference on the certification documents is clearly stated as being only a control set source for controls applied in the Statement of Applicability and not a certification thereof.

## CHAPTER 5 RECERTIFICATION

**5.1**

At the time of the Management System recertification audit, scheduled every three years, the organization must send RINA the application form and the specific **ANNEX TO THE APPLICATION FORM FOR THE ISO/IEC 27001 (ISMS) and ISO/IEC 27XXX:20YY**, available on the RINA web site www.rina.org. The two documents must be duly filled in as described in paragraph 3.1 of this regulation.

## CHAPTER 6 CONDUCTING THE AUDIT

### 6.1 INTRODUCTION

**6.1.1**

The guidelines extension audit must be completely carried out at the organization's site(s), including the datacenter(s) hosting the ICT infrastructure, as described in paragraph 3.5 of this regulation.

On-site audit time must be at least 70% of the total audit time.

The audit for organizations with integration to the guidelines will include a verification of the Statement of Applicability (SoA) regarding the specific controls defined in the guidelines, new or modified, chosen by the organization.

## CHAPTER 9 MULTISITE ORGANIZATIONS SPECIAL FEATURES

**9.1**

Site sampling to conduct the audit may also include the datacenter(s) hosting the organization's ICT infrastructure. RINA will evaluate the applicability of the sampling process according to the **General Regulation for the Management Systems Certification** and according to the following elements:

- the central function and site(s) internal audits results or the audit results of past certification audits;
- the Management System complexity;
- the site(s)'s IT system complexity;
- potential interactions with critical IT system(s) or with sites managing sensitive data;
- the risk evaluation;

The organization's central function must partake to the security policy definition and management, to the risk evaluation, the analysis and processing, definition, management and analysis of the controls, definition and management of the Statement of Applicability.

## CHAPTER 10 ACCREDITED CERTIFICATES TRANSFER

**10.1**

If an organization with a valid certification issued by another management systems certification body that is accredited by an accreditation organization signatory of the IAF/MLA would like to transfer its own certification to RINA, the organization must send RINA the application form and the specific **ANNEX TO THE APPLICATION FORM FOR THE ISO/IEC 27001 (ISMS) AND ISO/IEC 27XXX:20YY**, that is available on the RINA web site www.rina.org. The documents must be duly filled in as described in paragraph 3.1 of this regulation, together with a copy of the Management System certificate, and a copy of the Statement of Applicability whose references are also included on the certificate itself.

# SECTION 3: TRANSITION OF CERTIFICATION FROM ISO/IEC 27001: 2013 (UNI CEI EN ISO/IEC 27001:2017) TO ISO/IEC 27001: 2022

## A.0 INTRODUCTION

This section applies when an Organization in possession of a certification issued for compliance with ISO/IEC 27001: 2013 (UNI CEI EN ISO/IEC 27001: 2017), requests the passage of certification to the edition of ISO/IEC 27001: 2022, hereinafter referred to as "transition" and defines the additional and/or replacement procedures applied by RINA for the certification of Information Security Management Systems with respect to what is already defined in the:

**General Regulation for the certification of Management Systems**.

The points of this section of the Regulation refer to and maintain the same numbering of the corresponding points of the General Regulations for the Certification of Management Systems for which amendments and/or additions have been made.

To obtain the certification by RINA to the new revision of the standard, an Information Security Management System must initially meet the requirements of ISO/IEC 27001: 2022 in addition to those defined in the General Regulation for the certification of Management Systems.

## 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 27001:2022 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.

# Information Security Management Systems Certification Regulation and extension to guidelines ISO/IEC 27XXX

Publication: RC/C 56
English edition

RINA
Via Corsica 12
I-16128 Genoa - Italy

Phone # +39 010 53851 Fax
# +39 010 5351000
website www.rina.org

---

Technical regulations