
Valid from 20th October 2020

RINA
Via Corsica 12
I-16128 Genoa - Italy

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

Technical regulations
# TABLE OF CONTENT

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHAPTER 1 INTRODUCTION</td>
<td>3</td>
</tr>
<tr>
<td>CHAPTER 3 FIRST CERTIFICATION</td>
<td>3</td>
</tr>
<tr>
<td>CHAPTER 5 RECERTIFICATION</td>
<td>4</td>
</tr>
<tr>
<td>CHAPTER 6 CARRYING OUT THE AUDIT</td>
<td>4</td>
</tr>
<tr>
<td>CHAPTER 9 MULTISITE ORGANIZATIONS SPECIAL FEATURES</td>
<td>4</td>
</tr>
<tr>
<td>CHAPTER 10 ACCREDITED CERTIFICATES TRANSFER</td>
<td>5</td>
</tr>
</tbody>
</table>
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This document details which points of the Management System Certification General Regulation are superseded by this regulation.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 according to the requirements ISO/IEC 17021-1:2015 and ISO/IEC 27006:2015 only for organisation whose Management System has been declared compliant to every requirement of:


The certification can be integrated with the following guidelines:

ISO/IEC 27017: 2015
ISO/IEC 27018: 2019
ISO/IEC 27701: 2019

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 Organisation 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 organisation 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 organisation 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.

CHAPTER 3
FIRST CERTIFICATION

3.1
The organisations 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) OFFER, 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:
• Datacentres where the servers managing the service are deployed / the sites hosting critical assets;
• Factors concerning the organisation 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 organisation’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 organisation’s site(s), including the datacentre(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 organisation and the supplier(s) will have to be examined and the operational controls in place.

CHAPTER 5
RECERTIFICATION

5.1

At the time of the Management System recertification audit, scheduled every three years, the organisation 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
CARRYING OUT THE AUDIT

6.1 INTRODUCTION

6.1.1

The guidelines extension audit must be completely carried out at the organisation’s site(s), including the datacentre(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.

CHAPTER 9
MULTISITE ORGANIZATIONS SPECIAL FEATURES

9.1

Site sampling to carry out the audit also includes the datacentre(s) hosting the organisation’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 organisation’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 organisation with a valid certification issued by another management systems certification body that is accredited by an accreditation organisation signatory of the IAF/MLA would like to transfer its own certification to RINA, the organisation 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 coordinates are also included on the certificate itself.
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