Rules for the certification of Information Security Management Systems

Effective from 14 November 2016

RINA
Via Corsica 12
16128 Genova - Italia

tel +39 010 53851
fax +39 010 5351000
web site : www.rina.org

Technical Rules

CONTENTS

CHAPTER 1
GENERAL

1.1

The present Rules define the additional, and not substitutive, procedures applied by RINA for the certification of Information Security Management Systems, in comparison with what is already defined in the:

Rules for the Certification of Management Systems

The points of these Rules refer (and keep the same numbering) to the corresponding points of the Rules for the Certification of Management Systems for which changes or integrations have been made.

1.2

Change to the General Rules:

"RINA issues the certification according to the requirements of the ISO/IEC 17021:2015 and ISO/IEC 27006:2015 to Organisations whose Management System . . . ."

1.7

Integration in the General Rules

The terminology used in these Rules is also indicated in the ISO/IEC 27001:2013.

CHAPTER 3
INITIAL CERTIFICATION

3.1

Integration to the General Rules

Organisations wishing to obtain certification for their Information Security Management System must also provide RINA with their main organisation/production data and site location by filling in all parts of the "Informative Questionnaire" form, and the specific "Annex To Informative Questionnaire for ISO/IEC 27001 (ISMS Certification)" available at www.rina.org, and sending it to RINA which will use it to prepare a quotation.

In particular, the Organisation must also inform RINA

if the Information Security Management System includes documentation (procedures, records, etc.) classified as "confidential" and/or in any case not available for certification purposes. RINA will then assess whether the conditions are right to continue the certification process.

CHAPTER 6
PERFORMANCE OF AUDITS

6.2.1

Integration in the General Rules

The purpose of the stage 1 audit is also to:

- check whether the risk assessment, plan for dealing with risk and the statement of applicability (and any declared exclusions) are suitable in relation to the organisation's field of application and activities
- check whether the outsourced activities have been adequately identified and monitored, confirming, if necessary, the need to perform an audit at third parties.

Stage 1 is usually performed at the customer's premises, preferably at its head office or in any case at a site included in the certification scope and where the stage 2 audit will be carried out. It may be foreseen that in particular cases, evaluated on a case by case basis by RINA, part of the stage 1 phase need not be carried out at the organisation's premises.

CHAPTER 7
MANAGEMENT OF CERTIFICATES OF CONFORMITY

7.1

Integration in the General Rules

The certificates issued make reference to the Statement of Applicability, its edition and date of issue, in force during the audits carried out at the organisation's premises.

CHAPTER 9
SPECIAL REQUIREMENTS FOR MULTI-SITE ORGANISATIONS

9.1

Integration in the General Rules

At least the following activities must also be managed by the central function of the organisation:

- definition and management of the security policy
- risk assessment, analysis and treatment
- definition and management of controls
- definition and management of the statement of applicability

assessment of training requirements.

9.2

Integration to the General Rules:

"If the organisation observes the previous requirements, RINA always checks the feasibility of sampling on all the sites and may decide whether to limit this sampling in the presence of:

- the results of the internal audits of the head office and of the sites or of previous certification audits;
- complexity of the ISMS;
- complexity of the IT systems at the various sites;
- potential interaction with critical IT systems or with IT systems which manage sensitive information;
- risk assessment.

CHAPTER 10
TRANSFER OF ACCREDITED CERTIFICATES

10.1

Integration in the General Rules

The organisation, if it accepts the economic offer, must send RINA the "Certification request" together with the following documents:

- controlled copy of the Statement of Applicability referred in the Certificate.

Rules for the certification of Information Security Management Systems

Publication: RC/C 56

English edition

RINA
Via Corsica 12
16128 Genova - Italia

tel +39 010 53851
fax +39 010 5351000
web site : www.rina.org

Technical Rules