



**RINA**

**Rules for the certification of  
Information Security Management Systems**

# **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](http://www.rina.org)**

---

**Technical Rules**



RINA

## Rules for the certification of Information Security Management Systems

### CONTENTS

CHAPTER 1: GENERAL

CHAPTER 3: INITIAL CERTIFICATION

CHAPTER 6: PERFORMANCE OF AUDITS

CHAPTER 7: MANAGEMENT OF CERTIFICATES OF CONFORMITY

CHAPTER 9: SPECIAL REQUIREMENTS FOR MULTI-SITE ORGANISATIONS

CHAPTER 10: TRANSFER OF ACCREDITED CERTIFICATES



RINA

## Rules for the certification of Information Security Management Systems

### 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](http://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.



RINA

## Rules for the certification of Information Security Management Systems

### 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



RINA

## Rules for the certification of Information Security Management Systems

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](http://www.rina.org)

---

Technical Rules



**RINA**

**Regolamento per la certificazione di  
Sistemi di Gestione della Sicurezza delle Informazioni**

# **Regolamento per la certificazione di Sistemi di Gestione della Sicurezza delle Informazioni**

*In vigore dal 14 Novembre 2016*

**RINA**  
**Via Corsica 12**  
**16128 Genova - Italia**

**tel +39 010 53851**  
**fax +39 010 5351000**  
**web site : [www.rina.org](http://www.rina.org)**

---

**Regolamenti tecnici**



RINA

## Regolamento per la certificazione di Sistemi di Gestione della Sicurezza delle Informazioni

### INDICE

CAPITOLO 1: GENERALITA'

CAPITOLO 3: CERTIFICAZIONE INIZIALE

CAPITOLO 6: ESECUZIONE DEGLI AUDIT

CAPITOLO 7: GESTIONE DEI CERTIFICATI DI CONFORMITA'

CAPITOLO 9: PARTICOLARITA' PER ORGANIZZAZIONI MULTISITO

CAPITOLO 10: TRASFERIMENTO DI CERTIFICATI ACCREDITATI





RINA

## Regolamento per la certificazione di Sistemi di Gestione della Sicurezza delle Informazioni

### CAPITOLO 1 GENERALITA'

#### 1.1

Nel presente Regolamento sono definite le procedure supplementari, e non sostitutiva, applicate da RINA per la certificazione di Sistemi di Gestione della Sicurezza delle Informazioni rispetto a quanto già definito nel:

Regolamento Generale per la certificazione di Sistemi di Gestione

I punti del presente Regolamento si riferiscono (e mantengono la stessa numerazione) ai punti corrispondenti del Regolamento Generale per la Certificazione di Sistemi di Gestione per i quali sono state apportate modifiche e/o integrazioni.

#### 1.2

Modifica al Regolamento Generale:

“RINA rilascia la certificazione in accordo ai requisiti della norma ISO/IEC 17021:2015 e ISO/IEC 27006:2015 ad Organizzazioni il cui Sistema di Gestione . . . . .”

#### 1.7

Integrazione al Regolamento Generale:

La terminologia usata nel presente Regolamento è quella riportata nella norma ISO/IEC 27001:2013.

### CAPITOLO 3 CERTIFICAZIONE INIZIALE

#### 3.1

Integrazione al Regolamento Generale:

Le Organizzazioni che desiderino ottenere la certificazione del loro Sistema di Gestione della Sicurezza delle Informazioni devono fornire a RINA i dati essenziali della loro Organizzazione e relative attività svolte e la localizzazione del Sito/i, inviando l'apposito modulo “Questionario Informativo” compilato in tutte le sue parti e lo specifico “Allegato al Questionario Informativo per ISO/IEC 27001 (Certificazione ISMS)” disponibili sul sito [www.rina.org](http://www.rina.org), sulla base dei quali viene formulata da RINA un'offerta economica.

In particolare, l'Organizzazione deve comunicare a RINA:

se il Sistema di Gestione della Sicurezza delle informazioni comprenda documentazione (procedure, registrazioni, ecc.) classificata come “riservata” e/o comunque non disponibile ai fini della certificazione. RINA valuterà conseguentemente la sussistenza delle condizioni per poter proseguire l'iter di certificazione.



**RINA**

## **Regolamento per la certificazione di Sistemi di Gestione della Sicurezza delle Informazioni**

### **CAPITOLO 6 ESECUZIONE DEGLI AUDIT**

#### 6.2.1

Integrazione al Regolamento Generale:

Lo scopo dello Stage 1 è anche:

- verificare se l'analisi del rischio, il piano di gestione del rischio e la Dichiarazione di Applicabilità (e qualunque esclusione dichiarata) sia adeguata rispetto al campo di applicazione e alle attività dell'Organizzazione
- verificare se le attività esternalizzate sono state identificate in modo adeguato e monitorate, confermando, se necessario, la necessità di condurre un audit presso le terze parti.

Lo Stage 1 è solitamente condotto presso il sito dell'organizzazione preferibilmente presso il sito principale e in ogni caso presso un sito compreso nell'ambito di certificazione e dove lo Stage 2 sarà condotto. Potrebbe essere previsto che in casi particolari, da valutare caso per caso da parte del RINA, una parte dello Stage 1 non sia condotta presso i siti dell'organizzazione.

### **CAPITOLO 7 GESTIONE DEI CERTIFICATI DI CONFORMITA'**

#### 7.1

Integrazione al Regolamento Generale:

Il certificato emesso fa riferimento alla Dichiarazione di Applicabilità, la sua versione e data di emissione, in vigore durante l'audit condotto presso i siti dell'Organizzazione.

### **CAPITOLO 9 PARTICOLARITA' PER ORGANIZZAZIONI MULTISITO**

#### 9.1

Integrazione al Regolamento Generale:

Almeno le seguenti attività devono essere anche gestite dalla funzione centrale dell'Organizzazione:

- definizione e gestione della politica di sicurezza;
- valutazione del rischio, analisi e trattamento;
- definizione, gestione e analisi dei controlli;



**RINA**

## **Regolamento per la certificazione di Sistemi di Gestione della Sicurezza delle Informazioni**

- definizione e gestione della Dichiarazione di Applicabilità;
- verifica dei requisiti di formazione.

### 9.2

Integrazione al Regolamento Generale:

“Se l'Organizzazione rispetta i requisiti precedenti, RINA verifica sempre l'applicabilità del campionamento su tutti i siti e può decidere se limitare il campionamento in presenza di:

- i risultati degli audit interni della sede centrale e dei siti o di precedenti audit di certificazione;
- complessità del ISMS ;
- complessità dei sistemi IT dei diversi siti;
- potenziale interazione con i sistemi IT critici o con i sistemi IT che gestiscono dati sensibili;
- la valutazione del rischio.

## **CAPITOLO 10 TRASFERIMENTO DI CERTIFICATI ACCREDITATI**

### 10.1

Integrazione al Regolamento Generale:

L'Organizzazione, se accetta l'offerta economica, deve inviare a RINA la Richiesta di certificazione" insieme ai seguenti documenti:

- copia controllata della Dichiarazione di Applicabilità riportata nel Certificato.



RINA

## **Regolamento per la certificazione di Sistemi di Gestione della Sicurezza delle Informazioni**

Publicazione: RC/C 56

Edizione Italiana

RINA  
Via Corsica 12  
16128 Genova - Italia

tel +39 010 53851  
fax +39 010 5351000  
web site : [www.rina.org](http://www.rina.org)

---

Regolamenti tecnici