Rules for the certification of Security Management Systems

Effective from July 1st, 2009

RINA Società per azioni
Via Corsica, 12 - 16128 Genova - Italy
Tel.: +39 01053851 - Fax: +39 0105351000
www.rina.org

Technical regulations

CONTENTS

CHAPTER 1
GENERAL

1.1

These Rules describe the procedures applied by RINA for the certification of Security Management Systems (SMS) and how organisations can apply for, obtain, retain and use this certification, as well as its possible suspension and revocation.

For any issues not covered in this document, reference should be made to "GENERAL CONTRACT CONDITIONS GOVERNING SYSTEM, PRODUCT AND STAFF CERTIFICATION" which can be downloaded at www.rina.org.

1.2

RINA issues this certificate to organisations whose Security Management System has been recognised as fully conforming to the ISO 28000:2007 standard.

1.3

Certification is open to all Organisations and does not depend on whether they belong to an association or group.

RINA will apply the fees established on the basis of its current tariffs for the certification service and guarantees fairness and uniformity of application. RINA is entitled to refuse requests for certification by organisations that have been the subject, or whose production or activities have been the subject, of restriction, suspension or proscription by a public authority.

1.4

The certificate issued by RINA pertains exclusively to a single organisation, where organisation means a group, company, enterprise, body or institution, or parts and combinations thereof, whether associated or not, public or private, with its own functional and administrative structure.

For organisations with more than one operating unit, a single operating unit can be defined as an organisation.

1.5

The procedures envisaged in these rules are also applied when Security Management System certification is requested under the provisions of the RINA Rules for the classification of ships or other rules applicable to the organisation; in such cases, any additional requirements for the Security System contained therein are to be complied with.

1.6

The terminology used in these Rules is indicated UNI CEI EN ISO/IEC 17000:2005 standards.

1.7

RINA ensures that all the members of the Audit Team work according to the RINA policy regarding the confidentiality of the information obtained during the audit activities. Information about a client will not be disclosed to a third party without the written consent of the client/individual concerned.

RINA ensures secure handling of confidential information (e.g. documents, records) and adequate control of the identification, storage, protection, retention time and disposition of its records related to fulfilling the requirements of the ISO 28000:2007 standard.

RINA security auditors will be subject to a background investigation and will have to demonstrate their security clearance.

CHAPTER 2
REFERENCE STANDARD / CERTIFICATION REQUIREMENTS

2.1

Organisations wishing to obtain RINA certification of their Security Management System must first and henceforth satisfy the requirements of ISO 28000:2007.

An organisation is to establish, document, implement, maintain and continually improve an effective security management system to identify security threats, assess risks and control and mitigate their consequences. The effectiveness of the implemented system is to be improved according to the requirements defined in §4 of the ISO 28000:2007 standard.

2.2

In particular, in order to obtain Security Management System certification, the organisation must:

2.2.1. have established a Security Management System and kept it active in total compliance with the requirements of the required standard. A Security Management System is considered as being fully operative when:

- it has been applied for at least three months,
- the internal audit system has been fully implemented and its effectiveness can be demonstrated,
- at least one management review of the system has been carried out and documented,
- the objectives and processes required to obtain results in agreement with customer requirements and company security policy have been defined,
- these processes have been developed,

- monitoring activities and measurements of the processes and products with respect to the product objectives and requirements have been performed and registered,
- actions have been implemented to promote continual process improvement and guarantee constancy in production methods and in the quality of the products or services supplied.

2.2.2. Have prepared a manual:

- defining the goal/scope of the Security Management System, describing the main processes and their interactions and containing or referring to the relative documented procedures.
  The description of the processes and their interactions must be extended to all those developed by the Organisation (also to outsourced processes) required to manufacture/provide a determined product/service that are determining as regards the capacity of the product/service to satisfy the applicable requirements).
  This can be done in various ways:
  - Descriptions
  - Flow charts or logograms
  - Tables or matrices
  - Other
- taking into consideration the requirements of the standard and giving a description, not necessarily detailed, of the resources and procedures used to ensure compliance with these requirements,
- specifying security management policy,
- containing a suitable description of the company Organisation.

2.2.3. Have prepared adequate procedures:

- For the ongoing identification and assessment of security threats and security management-related threats and risks
- For the identification and implementation of necessary management control measures
- For specific security training for the employees.

2.3

The requirements indicated in point 2.2 are verified by RINA by means of a two-stage initial audit:

- Audit stage 1. RINA carries out preliminary checks, generally at clients' premises;
- Audit stage 2. RINA carries out an on-site audit.

The special features of the initial audit are described in the next chapter.

CHAPTER 3
INITIAL CERTIFICATION

3.1

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

In particular, the organisation must inform RINA of:

- any aspects of the reference standard which it considers to be inapplicable or which required interpretation or adaptation, clearly stating the reasons for this;
- information concerning all the processes outsourced by the organisation that may affect conformity with requirements;
- the number of permanent and temporary sites involved in certification and the relative activities carried out there.

This information is required in order to verify the application of certain requirements of the standard beforehand and to draw up a suitable offer.

If organisations accept RINA's quotation, they must make their application official by sending RINA the specific form attached to the offer, indicating the reference standard and, if relevant, any other reference standard document according to which certification is requested.

On receipt of the application for certification and the relative annexes and having ensured they are complete, RINA will send the organisation written acceptance of its application.

The organisation's request, which makes specific mention of these rules, and its acceptance by RINA, contractually formalise the relationship between RINA and the organisation, and the applicability of these rules.

The agreement signed between RINA and the organisation includes:

- the initial audit comprising two stages and the issue of the certificate;
- subsequent surveillance and recertification audits
- any additional services specified in the offer.

RINA will notify the Organisation of the names of the qualified auditors who will carry out the stage 1 audit and the stage 2 audit; the Organisation may object to the appointment of these surveyors, giving its reasons.

During the initial audit, the organisation must be able to demonstrate that the Management System has been fully operational for at least three months and that it effectively applies the system and relative documented procedures.

3.2

Together with or following the certification request, the Organisation has to present RINA the following documents:

- security management manual (the most recent valid revision);
- a list of internal security procedures;
- copy of the Chamber of Commerce registration certificate or an equivalent document, certifying the existence of the Organisation and describing the activity it performs;
- Organisation chart of the Organisation's Management System;
- site plan/s;
- latest Management Review;
- Internal Audit planning, focused on security aspects;
- a list of the main laws and/or regulations applicable to the product/service provided;
- list of current operational yards, describing the activities performed there.

RINA may ask, at its discretion, to examine other documents, apart from those previously mentioned, that are considered to be important for assessing the Security Management System.

RINA examined the above documents for conformity with the reference standard and with the requirements of these Rules.

3.3

The stage 1 audit is to be performed

- to audit the client's Security Management System documentation;
- to evaluate the client's location and site-specific conditions and to undertake discussions with the client's personnel to determine the preparedness for the stage 2 audit;
- to review the client's status and understanding regarding requirements of the standard, in particular with respect to the identification of key performance or significant aspects, processes, objectives and operation of the Security Management System;
- to collect the necessary information regarding the implemented security processes and location(s) of the client and related statutory and regulatory aspects and compliance

- to review the allocation of resources for the stage 2 audit and agree with the client on the details of the stage 2 audit;
- to provide a focus for planning the stage 2 audit by gaining a sufficient understanding of the client's Security Management System and site operations in the context of possible significant aspects;
- to evaluate if the internal audits and management review are being planned and performed and that the level of implementation of the Security Management System substantiates that the client is ready for the stage 2 audit.

The outcome of the stage 1 audit is communicated to the Organisation by sending a copy of the stage 1 audit report which, among other things, indicates any observations found, including those that could be classified as non-conformities during the stage 2 audit.

The actions taken by the organisation to eliminate these observations are generally checked during the audit stage 2 referred to in point 3.4.

In the event of observations deemed to be particularly important, in the judgement of the surveyors who performed the audit, the organisation may be required to totally eliminate them before the audit stage 2 takes place.

Normally, the stage 1 audit is performed at the Organisation's premises.

3.4

The audit stage 2 is conducted at the organisation following the successful outcome of the stage 1 audit as described in point 3.3, in order to verify the correct implementation of the Security Management System.

Before conducting the audit stage 2, RINA sends an audit plan to the site/s of the organisation giving a detailed description of the activities and the requirements for conducting the audit.

If the organisation performs its activities on more than one operative site, the audit will be performed according to criteria established by RINA and communicated to the Organisation.

This audit is performed by qualified RINA surveyors, on the basis of the stage 1 audit and the following updated documents prepared by the organisation:

- Security Management System Manual,
- informative questionnaire filled in by the Organisation,
- list of internal security procedures,
- other relevant Security Management System documents.

The audit stage 2 essentially comprises:

- an initial meeting with the technicians of the organisation in order to agree and confirm the audit objectives and methods indicated in the audit plan;
- verification that the corrective actions relative to the observations found during the audit stage 1 have been effectively implemented;
- an inspection of the production site/s of the organisation to verify conformity of the Security Management System with the reference documents and its complete implementation;
- a closing meeting to explain the outcome of the audit.

3.5

At the end of the audit stage 2, the organisation is given an audit report containing any non-conformities found as well as any recommendations.

The organisation may indicate any reservations or observations concerning the findings by the RINA surveyors in the relative space in the audit report.

The contents of this report are subsequently confirmed by RINA in writing.

If there is no written communication from RINA, the report is to be considered as confirmed three days after being received by the organisation.

After analysing the reasons for any non-conformities indicated in the above report, the Organisation must, within the data indicated on the report, inform RINA of its proposals for handling the non-conformities, as well as the corrective action required and the dates envisaged for its implementation.

The "Member Area" of the RINA website (www.rina.org) can be used to send handling and corrective action proposals to RINA for acceptance.

The organisation, in fact, may propose handling methods and corrective action by filling in the relative forms directly in the "Member Area" of the RINA website (www.rina.org).[1]

RINA will notify the organisation in writing of acceptance of the proposals and of the relative implementation deadlines.

3.6

In the event of serious non-conformities[2] the certification process is suspended; in the event of other findings, the number of which, in the audit team's judgement, may compromise the efficiency of the system, the certification process is also suspended.

[1] If it is impossible to access the Internet, the organisation may fill in a paper form and send it to the pertinent RINA Office.

[2] "Serious non-conformities" mean:
- total non-observance of one or more reference standard requirements;
- non-compliance with one or more requirements of these Rules;
- situations that could cause serious shortcomings in the management system or reduce its capacity to ensure the control of Security aspects/impacts and/or compliance with legislation.

In these cases, a supplementary audit is to be performed within three months in order to ascertain whether the proposed corrective action has been taken; if this audit is successful the certification process will be resumed.

The auditing team may decide to perform the supplementary audit on site or on the documents, depending on the type of corrective action involved.

If the above period is exceeded, the Security Management System is completely re-examined within six months of the finding.

After the six month period has elapsed with no positive outcome of the assessment, RINA reserves the right to definitively close the certification file and charge the time spent and expenses incurred up to that moment. In such a case, if the Organisation wishes to proceed with RINA certification, it must submit a new application and repeat the certification procedure.

In special cases, the above time limits may be modified at the request of the organisation, if considered justified by RINA.

3.7

After the satisfactory completion of the evaluation and validation by the relative RINA committee, a Certificate of Conformity of the Security Management System, valid for three years, will be issued (the facsimile of which is available at www.rina.org).

The validity of the certificate is subject to the result of the subsequent annual surveillance audits and the three-yearly recertification of the Security Management System.

The frequency and extension of the subsequent audits for maintaining certification are established by RINA on a case-by-case basis by drawing up a three-year audit plan which it sends to the organisation.

For details on the management and validity of the certificates of conformity issued by RINA, see chapter 6.

CHAPTER 4
MAINTENANCE OF CERTIFICATION

4.1

The organisation must ensure its Security Management System continues to comply with the Reference Standards.

4.2

The Organisation must record any claims and the relative corrective action implemented and must make these records available to RINA together with the corrective action implemented during the periodic audits.

4.3

RINA performs periodic audits on the Security Management System in order to evaluate whether it remains compliant with the requirements of the reference standard.

Certification maintenance audits are divided into two types:

- surveillance audits, generally performed at least once a year.
  The Organisation must record any claims and the relative corrective action implemented and must make these records available to RINA together with the corrective action implemented during the periodic audits.
- recertification audit (see charter 5);
  The Security Management System must be totally reviewed every three years.

4.4

Surveillance audits are performed at the organisation's site/s, according to a three-year programme which enables each item contained in the reference standard according to which the Security Management System was certified to be audited at least once during the three years of validity of the Certificate.

The following aspects will be considered during the surveillance audits:

a) internal audits and management reviews;

b) a review of the action taken as a result of the non-conformities identified during the previous audit;

c) handling claims;

d) the effectiveness of the Management System in achieving objectives;

e) the progress of activities implemented to promote continual improvement;

f) continual operative control;

g) a review of any changes.

Details of the activities and instructions for performing surveillance audits at the site/s are described in the surveillance audit plan which RINA sends to the organisation before performing the audit.

4.5

At least one surveillance audit must be performed at intervals of not more than 12 months and the date within which the audits must be performed is indicated on the three yearly audit plan sent to the organisation.

This programme may be modified by RINA according to the results of the previous surveillance audits.

If the limits of the surveillance audits are exceeded for justified reasons, this must be agreed in advance with RINA and recovered at the subsequent audit.

4.6

RINA also reserves the right to perform additional audits with respect to those established in three-year programme, announced or unannounced, at the organisation:

- if it receives claims or reports, considered to be particularly significant, relative to the non-compliance of the Security Management System with the requirements of the reference standard and of these Rules
- in relation to changes taking place in the organisation
- to organisations whose certification has been suspended.

If this is refused by the organisation without a justified reason, RINA may decide to suspend the certificate.

If RINA considers the claims and reports to be justified, the cost of the supplementary audit will be charged to the organisation.

4.7

The dates of the surveillance audits will be agreed with the organisation in due time and officially confirmed in writing.

The names of the side auditors appointed to perform the audits will be notified by RINA to the organisation which may object to the appointments, giving its reasons.

4.8

The outcome of the audits is notified as described in section 3.5.

The validity of the certificate is confirmed following the successful outcome of the surveillance audit.

4.9

In the case of serious non-conformities or other findings whose number in the opinion of the audit team is such as to impair the correct functioning of the system, the organisation will be subject to a supplementary audit within the time limits established by RINA in relation to the importance of the non-conformities and, in any case, not more than three months after the end of the audit.

If the non-conformities are not eliminated within the established times or if they prevent the control of Security aspects/impacts and applicable legal requirements, RINA may suspend certification until these non-conformities have been eliminated and, in any case, as specified in point 10.1.

All costs relative to any additional audits deriving from shortcomings in the Security Management System will be charged to the organisation.

CHAPTER 5
RECERTIFICATION

5.1

For the recertification audit of the Security Management System, performed every three years, the organisation must contact RINA about three months before the date indicated on the three-year audit plan in its possession, and send an updated and complete copy of the Informative Questionnaire (available at www.rina.org) in order to allow RINA to plan the activity and agree on the date of the recertification audit.

The date of the recertification audit will be agreed with the organisation in due time and officially confirmed in writing.

The names of the auditors appointed to perform the audits will be notified by RINA to the organisation which may object to the appointments, giving its reasons.

5.2

The recertification audit sets out to confirm maintenance of the conformity and effectiveness of the overall Management System and is mainly based on an audit to perform on-site, generally, using the same criteria as the audit stage 2.

In particular, the recertification audit comprises an on-site audit which considers, among other things, the following aspects:

a) the effective interaction between the processes of the Security Management System;
b) the effectiveness of the Security Management System in its entirety in the light of internal and external changes;
c) demonstrated commitment to maintain the effectiveness and improvement of the Security Management System in order to enhance overall performance;
d) that the operation of the certified s Security Management System contributes to the achievement of the organisation's policy and objectives.

Details of the activities and instructions for performing recertification audits at the site/s are described in the recertification audit plan which RINA sends to the organisation before performing the audit.

5.3

Following the successful outcome of the recertification audit, the auditing team submits a recertification proposal to RINA in order to allow it to reissue the certificate of conformity.

RINA reissues the certificate of conformity following the positive outcome of the assessment of the above proposal.

Confirmation of recertification approval by RINA with consequent issue of the certificate is sent to the organisation in writing.

For details on the management and validity of the certificates of conformity issued by RINA, see chapter 6.

5.4

The recertification procedure must be successfully terminated before the expiry date indicated on the certificate. This date cannot be extended by RINA.

Consequently, the recertification audit must be successfully terminated in sufficient time to allow RINA to approve the recertification proposal and reissue the certificate within the above date (at least one month before the expiry date of indicated on the certificate).

If it organisation fails to abide by the above deadlines and does not obtain the reissued certificate within the date of expiry, the certificate must be considered as expired starting from the day after the date of expiry indicated on the certificate.

Organisations intending to obtain certification following the expiry of the certificate must present a new application and, generally, repeat the entire initial certification procedure.

5.5

In the case of major non-conformities or other findings whose number in the opinion of the auditing team is such as to impair the correct functioning of the system, the organisation must effectively implement the relative handling and/or corrective action before the date of expiry of the certificate of conformity.

This means that the organisation must perform the supplementary audit to verify the elimination of these non-conformities in sufficient time for the subsequent issue of the certificate.

The established times within which the organisation must perform the supplementary audit are communicated to the organisation in the recertification audit report.

The auditing team may decide to perform the supplementary audit on site or on the documents, depending on the type of corrective action involved.

All costs relative to any additional audits deriving from shortcomings in the Security Management System will be charged to the organisation.

CHAPTER 6
MANAGEMENT OF CERTIFICATES OF CONFORMITY

6.1

The certificate of conformity issued by RINA is valid for three years starting from the date of approval by RINA of the initial certification or recertification proposal.

6.2

From the moment of issue of the certificate by RINA, an original copy of the same and of the relative three-year audit plan is made available to the organisation in the "Member Area" of the RINA website (www.rina.org). The organisation may therefore enter and download the above documents directly from this area of the RINA website.

If it is impossible to access the Internet, the organisation may request a hardcopy original from the pertinent RINA Office.

6.3

The validity of the certificate, throughout the three years of validity, is subject to the results of the subsequent surveillance audits.

The certificate of conformity is reissued following the successful outcome of each recertification audit within the established deadlines, as indicated in chapter 5 hereto.

The validity of the certificate may be suspended, withdrawn or relinquished in accordance with the contents of Chapters 10 and 11.

RINA directly publishes and updates the following on its website www.rina.org:

- the list of certified organisations;
- the status of validity of the certificates issued, indicating valid, suspended or invalid for each certificate;
- copies of valid certificates.

On request, RINA provides information on the reasons for the invalidity of the certificate.

CHAPTER 7
MODIFICATION TO CERTIFICATION AND COMMUNICATION OF CHANGES

7.1

An organisation in possession of certification may request a modification or extension by presenting a new certification application, accompanied by the duly updated documentation indicated in point 3.2. RINA reserves the right to examine requests on a case-by-case basis and to decide the evaluation methods for the purpose of issuing a new certificate according to the "GENERAL CONTRACT CONDITIONS GOVERNING SYSTEM, PRODUCT AND STAFF CERTIFICATION" and ISO 28003:2007 standard.

7.2

The organisation must promptly inform RINA of any changes in factors that may affect the capacity of the Management System to continue to satisfy the requirements of the standard used for certification.

This requirement concerns, for example, modifications to:

a) the legal, commercial, organisational or ownership status;
b) organisation and management (e.g.: key managers or technical staff, decision-making process);
c) contact addresses and sites;
d) field of application of the activities covered by the certified management system;
e) significant changes in the management system and processes.

RINA reserves the right to perform additional audits on the organisation if the modifications communicated are considered particularly significant as regards maintaining the conformity of the Security Management System with the requirements of the reference standard and of these Rules or to review the economic conditions for the possible modification of the contract.

CHAPTER 8
SPECIAL PROCEDURES FOR MULTI-SITE ORGANISATIONS

8.1

Generally, all the sites of the Organisation are to be audited. Deviations from the man/days audit durations described in Annex A of the ISO 28003:2007 Standard are to be justified, based on a risk management approach defined by RINA, considering the scope sectors or activities, type and size of the sites eligible for multiple site assessment, variations in the local implementation of the Security Management System and use of temporary sites which operate under the Security Management System of the organisation.

If an organisation works on more than one permanent site, all the functions pertaining to the Security Management System are managed from a head office and a single certificate is requested, the audit man days can be reduced for some of the sites, as long as:

- the supply chain services provided by all the sites and all activities are substantially the same and are carried out fully in accordance with the same methods and procedures
- a common Security Management System is implemented for all sites and the Organisation has implemented the corrective actions, when needed, in all sites;
- the security threats are the same for each operational site and the Organisation has carried out a threat and risk assessment for each site and implemented operational controls accordingly;
- at least the following activities are managed by the head office of the Organisation:

- management review;
- improvement objectives, targets and management programmes;
- assessment of training requirements;
- control and modification of documents;
- evaluation of complaints, incidents, corrective and preventive actions;
- planning/execution of internal audits and assessment of results;

- Before the initial audit by RINA, the organisation performs an internal audit on each site and, following completion of any corrective action, assesses its conformity with the reference standard. The Organisation should be able to demonstrate, through records, the effectiveness of the controls for all the sites including those not subject to certification/registration body audits.

8.2

RINA issues a single certificate with the name and address of the headquarters of the organisation. A list of all the sites to which the certificate refers is indicated in an annex or on the certificate.

The Organisation may be issued with a certificate extract for each site covered by certification, provided it indicates the same purpose or a sub-element, and includes a clear reference to the main certificate.

8.3

For any non-conformities found on one site during audits, the organisation must evaluate whether they are due to shortcomings common to more than one site and, if so, it must adopt corrective action both at the headquarters and at the other sites.

8.4

On the basis of the information provided by the organisation, RINA establishes sampling plans that are applicable both to surveillance and recertification audits. The number of sites subject to sampling for each scheduled audit is indicated in the three-year audit plan.

CHAPTER 9
TRANSFER OF CERTIFICATES

9.1

If an Organisation with a valid certificate issued by another body presents a certification application, RINA proceeds as follows:

- documents review as indicated in paragraph 3.2 of these rules;

- review of the reports of the previous audits performed by the accredited body that issued the previous certification;
- possible audit at the organisation, the scope of which depends on the conformity and validity of the previously issued certification

The organisation must also inform RINA of:

- the reasons for the certificate transfer request
- any observations or reports by national or local authorities;
- any claims received and relative action taken

The contract between RINA and the applicant is managed as indicated in paragraph 3.1, depending on the scope of auditing activities.

After the satisfactory completion of the above activities a Certificate of Conformity of the Security Management System is issued which generally maintains the deadline established by the body which issued the previous certificate.

Generally speaking, surveillance and recertification audits are also performed according to the plan established by the organisation that issued the previous certificate.

CHAPTER 10
SUSPENSION, RENEWAL AND WITHDRAWAL OF CERTIFICATION

10.1

The validity of the certificate of conformity may be suspended as indicated in "GENERAL CONTRACT CONDITIONS GOVERNING SYSTEM, PRODUCT AND STAFF CERTIFICATION" and in the following specific cases:

- if the organisation does not allow surveillance or recertification audits to be performed at the requested frequencies;
- if serious non-conformities are found in the Security Management System which have not been corrected within the time limits established by RINA
- if the organisation does not observe the deadlines established for the communication of corrective actions, following non-conformities indicated on the audit report;
- if the organisation has made far-reaching changes to its Site/s or moves to another site without informing RINA of such changes
- if the organisation has made modifications to its Security Management System that have not been accepted by RINA;

- if the organisation has undergone important re-structuring and has not reported this to RINA;
- for evidence that the Security Management System does not guarantee the respect of the laws and regulations applicable to the activity and/or the site/s;
- if justified and serious claims received by RINA are confirmed.

The Organisation may also make a justified request to suspend certification, normally for not more than six months and in any case not after the expiry date of the certificate.

This suspension will be notified to the organisation in writing, stating the conditions for re-instating certification and the date by which the new conditions are to be complied with.

Suspension of the validity of the certificate is made public by RINA directly on the website www.rina.org as indicated in point 6.3.

10.2

Reinstatement of certification is subject to verification that the shortcomings which led to the suspension itself have been eliminated. This is achieved by means of an analytical audit checking the compliance of the Security Management System with all the requirements of the reference standard.

It is notified to the organisation in writing and made public by RINA on its website www.rina.org as established in point 6.3.

10.3

Failure to fulfil the conditions as per point 10.2 above by the established date will lead to revocation of the Certificate of Conformity.

Revocation of the certificate of conformity may be decided as indicated in "GENERAL CONTRACT CONDITIONS GOVERNING SYSTEM, PRODUCT AND STAFF CERTIFICATION" and in the following specific cases:

- when there are reasons such as those indicated in point 10.1 for suspension, which are held to be particularly serious;
- if the organisation stops the activities or services covered by the certified Security Management System for over six months as a rule;
- if the organisation does not accept the new economic conditions established by RINA due to a modification in the contract;
- for the case of multi-site organisations, if the headquarters or one of the sites does not comply with the criteria required to maintain certification;
- for any other reason that RINA deems to be serious.

Withdrawal of the Certificate of Conformity is notified in writing to the Organisation and made public by RINA as indicated in point 6.3.

Any Organisation which, following revocation of its Certificate, wishes to be re-certified, must submit a new application and follow the entire procedure all over again.

CHAPTER 11
RELINQUISHMENT OF CERTIFICATION

A certified organisation may send formal communication of withdrawal of certification to RINA, before the expiry of the certificate, including the case in which the organisation does not wish to or cannot conform to new provisions established by RINA.

Upon receipt of this communication, RINA starts the procedure for invalidating the certificate.

Generally speaking, within one month from the date of the communication, RINA updates the validity status of the certificate.

CHAPTER 12
CONTRACT CONDITIONS

For contract conditions, the contents of the current edition of RINA document "GENERAL CONTRACT CONDITIONS GOVERNING SYSTEM, PRODUCT AND STAFF CERTIFICATION" apply.

Publication: NC/C 64
English edition

RINA Società per azioni
Via Corsica, 12 - 16128 Genova - Italy
Tel. +39 01053851 - Fax: +39 0105351000
www.rina.org

Technical regulations