

✓
11/03/08

Statutory Notification (S.R.O)
Government of Pakistan
The Electronic Certification Accreditation Regulations
Information Security Auditors Registration, 2008

NOTIFICATION

Islamabad, the 11th March, 2008

SRO No. _____ .— In exercise of the powers conferred upon it under Section 43 read with Sections 21, 22, 24 and 25 of Electronic Transactions Ordinance 2002, the Certification Council hereby makes the following regulation:

1. Short title and commencement.— (1) These regulations shall be called as “Accredited Certification Service Provider’s Audit Regulations, 2008”

(2) These Regulations shall come into force at once.

2. Definitions.— (1) In these Regulations unless anything appearing repugnant to the context or subject:

a) “Accredited Certification Service Provider” means a Certification Service Provider accredited by the Council in pursuance of the Ordinance and under these Regulations;

b) “Approved Auditors List” means a list of Auditors having valid registration with the Council.”

c) “Audit” means information security assessment and evaluation of a Facility of a Certification Service Provider by an Auditor for grant or renewal of Accreditation Certificate to it by the Council in prescribed manner it includes Pre-Audit conducted under these Regulations;

d) "Auditor" means an approved auditor information security auditor holding a valid registration with the Council;

e) "Audit Report" means Audit report duly submitted by an Auditor in prescribed manner to the Council it includes Pre-Audit review report also;

f) "Authorized Officer" means an officer or group of officers of the Council including a member to whom the Council has delegated the exercise of any of its authority under the Ordinance;

g) "Certification Practice Statement" means the practice statement prepared under Section 25 of the Ordinance;

h) "Certification Service Provider" means a certification service provider who has not been accredited by the Council in pursuance of the Ordinance and under these Regulations;

i) "Council" means the council appointed by the Federal Government under Section 18(4) of the Ordinance;

j) "Facility" means principal place of business or any sub-office, site or location or any other place located any where in Pakistan or outside Pakistan wherein all or any of the system, data, electronic record and certificates are kept including all hardware equipment;

k) "General Surveillance Committee" means a surveillance committee constituted by the Council from time to time under Section 12 of these Regulations;

l) "Letter of Appointment" means letter issued by the Council appointing an Auditor to conduct an Audit of any or all Facilities of an Accredited Certification Service Provider or a Certification Service Provider and submit the Audit Report in prescribed time and manner;

m) "Monitoring Committee" means a committee constituted by the Council for any specified purposes under these Regulations;

n) "Ordinance" means Electronic Transactions Ordinance, 2002";

o) "Prescribed" means prescribed by these regulations or in any other regulations of the Council including their respective schedules and annexure; and

p) Scheduled Standards mean security standards adopted by the Council from time to time annexed with Schedule I of these Regulations.

(2) Words and expressions used in these Regulations and not defined but defined in the Ordinance shall have the same meaning specifically assigned to them in the Ordinance.

PART II

Application and Appointment of Auditor

3. Application for Appointment of Auditor .— (1) All Accredited Certification Service Provider shall apply to the Council in prescribed manner for appointment of an Auditor to get their all facilities audited annually to fulfil one of the conditions for renewals of their accreditation in prescribed manner from the Council.

Provided in case where the Council adopts any new Scheduled Standards the Accredited Certification Service Provider may delay the Audit for a maximum period of three months from the date of adoption of that new Scheduled Standards by the Council.

(2) Any Certification Service Provider may, at any time, apply to the Council in prescribed manner for Appointment of an Auditor to Audit its Facilities provided it must have up and running Facilities in place for at least six months prior to making any such application to the Council.

(3) In both the cases referred in Sub-Sections (1) and (2) the application shall be made in prescribed form and manner to the Council which shall contain:

- (i) purpose of application,
- (ii) brief profile of the applicant,
- (iii) brief description of the Facilities to be Audited,
- (iv) name of two proposed Auditors from the Approved Auditors List of the Council each one of whom in the opinion of the applicant is a suitable Auditor to Audit its Facilities, and
- (v) proof of payment of application processing fee in the prescribed manner.

4. Appointment of an Auditor.— (1) Upon receipt of an application for appointment of an Auditor under Regulation 3 the Council will appoint one Auditor out of the proposed Auditor which are proposed by the applicant or if the Council deems necessary then for reason to be recorded may appoint any other Auditor to audit the Facility of the applicant to conduct Audit and submit the Audit Report to the Council in prescribed manner.

(2) The Council shall appoint an Auditor with in seven days from the receipt of the application for the appointment of an Auditor.

(3) The decision of appointment of the Auditor under sub section 1 shall be communication in writing through a Letter of Appointment to the Auditor so appointed and to the applicant by the Council.

PART III

Audit

5. Initiation of Audit.— (1) Upon receipt of Letter of Appointment the Auditor shall within seven days initiate the process of Audit of the Facilities of the applicant and the Auditor may ask the Certification Service Provider or the Accredited Certification Service Provider as the case may be for any additional information which is deemed necessary to conduct the Audit.

(2) The Auditor shall duly inform in advance the day, time and place of initiation of the Audit to the Council and the Certification Service Provider or the Accredited Certification Service Provider as the case may be, in case there are more than one facilities to be Audited then the Auditor shall intimate about the exact date and time of his presence at each one of the facilities for the purpose of Audit.

6. Audit Requirements.— The Auditor shall carry out the Audit in prescribed manner in accordance with:

- (a) prescribed Scheduled Standards of the Council,
- (b) Certification Practice Statement;
- (d) any special directive issued by the Council in this regard.

7. Time limitations for Audit: The Audit shall be completed within 30 days from the date of initiation however, a time period of 15 days may be granted by the Council upon joint written request, containing reasons for extension of time, of the Auditor and the Accredited Certification Service Provider or the Certification Service Provider, as the case may be.

8. Audit Methodology:- (1) The Audit and assessment under these regulations shall comprise up of two stages:

- (i) Pre-audit review; and
- (ii) On-site Audit.

(2) In pre-audit review, the Auditor shall review the documents including Certification Practice Statement, processes and procedures employed with reference to Scheduled Standards, data logs, complaints logs, physical security standards of the Facility and other matters connected therewith for the purposes of providing an opportunity to the Accredited Certification Service Provider or Certification Service Provider, as the case may be, an opportunity to align its systems, procedures and processes in accordance with its Certification Practice Statement and Scheduled Standards.

(3) Notwithstanding any thing contained in these regulations, the Auditor shall submit the pre-audit review report directly to the Council and shall supply a copy to the Accredited Certification Service Provider or Certification Service Provider within the maximum period of 10 days of the start of pre-audit review.

Provided that the Report shall clearly mention the processes of pre-audit adopted by the Auditor by categorizing its findings and defects noted and steps suggested for rectification of shortcomings and lacunas.

(4) Notwithstanding anything contained in these regulations, the Auditor shall carry out the On-site Audit at the Facility and take into account at least, the following:

- (i) Confirmation to and adherence by the Accredited Certification Service Provider or the Certification Service Provider as the case may be to its own Certification Practice Statement; and
- (ii) Confirmation that the information security management system in the Facility conforms with the latest requirements and other standards recognized and included by the Council in its Scheduled Standards.

(5) The Accredited Certification Service Providers or the Certification Service Providers, as the case may be, shall facilitate and extend maximum cooperation to the Auditor to carry out the Audit of the Facility.

PART IV

Monitoring of Audit and Submission of the Audit Report

9. Council's right to monitor during Audit:- (1) The Council shall have right to inspect the Facility and monitor progress of the Audit with or without prior notice to the Accredited Certification Service Provider or Certification Service Provider or to the Auditor.

(2) The Council shall have right to enter and remain in the Facility and shall have right to inspect all the relevant data, processes and systems for the purposes of inspection and monitoring.

(3) The Council may constitute a Monitoring Committee by delegating its authority in writing to any of its members or employees for monitoring and inspection of the Facility during Audit.

(4) The Monitoring Committee shall have right to access and get extracts of any register, data log and any other information considered necessary for the evaluation of the Facility independent of the Audit and to monitor and assess the standards of the Audit itself. The Auditor, Accredited Certification Service Provider and the Certification Service Provider, as the case may be, shall extend maximum cooperation to the Monitoring Committee to carry out the inspection and monitoring of the Facility by the Council.

10. Submission of Report and actions taken by the Council: (1) The Auditor shall submit a duly signed and sealed Audit Report to the Council in the prescribed form and manner to ascertain:

i) the methodology adopted by the Auditor;

- ii) the fundamental facts and figures upon which the report is based;
- iii) the short falls the Auditor found out during the Audit;
- iv) the response and action taken by Accredited Certification Service Provider and Certification Service Provider upon pre-audit review;
- v) details of documents scrutinized; and
- vi) total time spent at the Facility.
- (vii) the details of the experts involved in the Audit.

(4) The Council shall have all the powers to raise queries to, or seek clarifications of, any fact arising out of the Audit report either from the Auditor or from the Accredited Certification Service Provider or the Certification Service Provider before accepting or rejecting the Audit Report.

12. Acceptance or Rejection of the Audit Report .—(1) The Council will have a right to accept or reject any Audit Report filled by an Auditor .

(2) When any Audit Report is rejected by the Council for reason to be recoded and after hearing the Auditor and the Accredited Certification Service Provider or the Certification Service Provider as the case may be, the Council will appoint an other Auditor for re-audit of the Facility at the cost of the Accredited Certification Service Provider or Certification Service Provider to submit the Audit Report with in 30 days or the Council will conduct the Audit by it self .

(3) In the event the Council decides to conduct the Audit by it self it will charge the Audit fee from the Accredited Certification Service Provider or the Certification Service Provider as the case may.

PART V
Fees and Fines

13. Fees.— (1) The Audit fee shall be negotiated and settled by the Auditor and the Accredited Certification Service Provider or the Certification Service Provider, as the case may be, the Auditor shall not charge more than range of the fee he intimated the Council

(2) Whoever apply to the Council for appointment of Auditor shall pay application processing fee along with the application as per Schedule of Fee.

(3) When even under the circumstances the Council decides to conduct an Audit it will charge a fee as per Schedule of Fee.

14. Fines.— (1) Notwithstanding anything contained in these regulations, whosoever contravenes the provisions of these Regulations by furnishing a wrong information to the or committing misrepresentation and prepare or get prepared an Audit Report on that basis, the Council may impose a fine which may extend to Rs. 10,000/- or the Council will lodge a criminal complaint against such person for fraud or misrepresentation as the case may be.

(2) Notwithstanding anything contained in these regulation, if an Auditor commits gross negligence while conducting an Audit or Pre-Audit or while submitting Audit Report to this effect to the Council or fails to provide an information required by these Regulations, the Council may impose a fine which may extend to Rs.15,000/-

Miscellaneous

15. Adoption of new Scheduled Standards .— In an event of adoption of any new standards as Scheduled Standards by the Council, the Accredited Certification Service Provider shall incorporate those new Scheduled Standards in its services within three months.

16. Appeals.— (1) Any party aggrieved by any order passed by and authorized officer or the Council under the provisions of these Regulations may within thirty days from the date of such order prefer an appeal to the Council.

(2) An appeal to any order of the Council shall lie to the Information and Communication Technologies Tribunal established under Section 31 of the Prevention of Electronic Crimes Ordinance, 2007.

Form A
(Application for Appointment of Auditor)
See Section 3

Name

Address

Purpose :Accreditation or Renewal of Accreditation

Profile of the Application

Facilities to be Audited

Proposed Auditors

Class Certification ----

Time of previous Audit

Reason of delay (if any)

Letter of Appointment

Name of the Auditor

Name of the Certification Service Provider

Date of Appointment

Time of Submission of Report

Form B

(for Submission of Audit Report to the Council)

- i) the methodology adopted by the Auditor;
- ii) the fundamental facts and figures upon which the report is based;
- iii) the short falls the Auditor found out during the Audit;
- iv) the response and action taken by Accredited Certification Service Provider and Certification Service Provider upon pre-audit review;
- v) details of documents scrutinized; and
- vi) total time spent at the Facility.
- (vii) the details of the experts involved in the Audit.

Sign and Seal of the Auditors

Undertaking

True and correct ,...Nothing is conceal ..etc