



professional training and certification

Course brochure

**Certified Internal Information Security  
Auditor  
(STQC – CIISA)**

**A program on ISMS internal auditing  
(based on standard ISO 27001)**

**March'14**



*Government of India  
Ministry of Communication & Information Technology  
Department of Electronic and Information Technology  
STQC Directorate*

Why STQC - CIISA?



The success of any business and effectiveness of business decisions depends largely on the availability and integrity of business information and the extent to which the information can be relied upon.

The information, therefore, is an asset to the organization needing adequate protection against unauthorized access, modification and removal. With advancement of information technology, the traditional methods of information management have been replaced with information management through IT enabled mechanisms such as maintenance of electronic files, databases, fast and easy access through computers, even from remote locations.

This has necessitated the need for advanced method for Information System Management System (ISMS). One of the means of determining effectiveness of ISMS in an organization is to carryout internal audits of ISMS. This three days training program aims in teaching ISMS Internal Audit techniques.

### Course objectives

The aim of this course is to provide participants with the knowledge and skills required to perform an internal audit of part of an information security management system based on ISO/IEC 27001 and report on the effective implementation and maintenance of the management system in accordance with ISO 19011.

### LEARNING OBJECTIVES

On completion, successful students will have the knowledge and skills to:

#### Knowledge

- Explain the process-based information security management system model for ISO/IEC 27001, and the role of internal audit in the maintenance and improvement of information security management systems.
- Explain the role and responsibilities of an auditor to plan, conduct, report and follow up an information security management system internal audit, in accordance with ISO 19011

#### Skills

- Plan, conduct, report and follow up an internal audit of part of an information security management system based on ISO/IEC 27001 and in accordance with ISO 19011

Note: The course references ISO/IEC 27001 as the management system standard that provides the context for the internal audit. However, this course does not address ISO/IEC 27001 in detail, and does not aim to equip participants with the knowledge and skills to determine conformity, or otherwise, with ISO/IEC 27001. Participants requiring the knowledge and skills to conduct entire information security management system audits against ISO 27001 should attend an ISMS Auditor/Lead Auditor training course.

### Course structure

- \* Introduction to ISMS and ISMS standards
- \* Overview of the requirements of ISO 27001
- \* Audit concepts
- \* Audit planning
- \* Audit execution
- \* Audit reporting
- \* Audit follow up and management



**For onsite program**, it is expected that the organization shall provide the participants access of its ISMS documented information including internal auditing, SoA, risk management; management review.

Course shall be concluded by an **examination** evaluating the understanding of participants regarding ISMS internal auditing, which is imparted in the program. Successful participants shall become STQC "Certified Internal Information Security Auditor" (STQC-CIISA)

### Who should attend?

- \* Persons responsible for conducting internal auditing of ISMS
- \* Persons responsible for implementation of ISMS
- \* Management system consultants,
- \* Information security officers
- \* IT Managers / System administrators / CIOs

### Pre-requisite

It is recommended that participants desirous to attend the STQC-CIISA program have the prior basic knowledge of the concepts of information security management system ISMS (see ISO/IEC 27000) and an understanding of the requirements of ISO/IEC 27001(with ISO/IEC 27002) and the commonly used information security management terms and definitions; (see ISO/IEC 27000).

### Course faculties:

Practicing ISO 27001 auditors, specifically trained for imparting knowledge & skill for auditing.

### Course details:

Participation	:	Maximum up to 20
Duration	:	3 days daily 0930h to 1730h (Local adjustments possible)
Material*	:	ISO standard (for training purpose), Course book (copy of projections), Exercise manual, Stationery
Fee	:	Local Contact course coordinator

\* For open programs only.

For **onsite programs**, one set of course material in .pdf format will be provided to the client. The client shall ensure distribution of course material in hard copy to each participant. For other requirements regarding availability of required standards and logistics please refer "Course logistics / infrastructure requirements for STQC-CIISA course".

Attendance on all days is compulsory.

Medium of course delivery shall be English.

### Certification:

Those who qualify the examination shall get STQC – CIISA qualifying certificates. Not qualified participants shall get participation certificates. They shall get one chance of re-sit in the STQC – CIISA examination within one year period from the date of commencement of program after paying an additional fee amount for re-sit examination.

## ABOUT STQC

STQC, is part of Department of Electronics & Information Technology, Govt. of India organization. STQC was set up in 1977 with an objective to improve the Quality of Indian Electronic and IT products & services and facilitate the industry to become global player. We have a nationwide network of 14 labs providing testing, calibration and certification services to industry.

In order to promote awareness, commitment and compliance to the recognized best IT practices, STQC has established eight IT centers all across the country at Kolkata, Mumbai, Delhi, Chennai, Bangalore, Hyderabad, Jaipur and Pune.

In the area of Information Security management, STQC is the first Indian accredited certification body in the country and first outside UK and Netherlands to offer Third party ISMS Certification as per ISO/IEC 27001:2013 . Our scheme is accredited from NABCB, Quality council of India .STQC is the National Certification Body under the Common Criteria for security testing of products. We also carry out, Risk Assessment/Gap Analysis (Readiness assessment) for interested organizations as part of their implementation of Information Security system as per ISO/IEC 27001 / ISO/IEC 27002 or any other standard. STQC has a team of competent ISMS auditors/ lead auditors duly qualified as per international requirements to accomplish these tasks.

STQC also provides education and training services in the form of public and tailor made onsite training courses covering aspects like

- IRCA Certified ISMS Lead Auditor Program
- STQC – CISP : A program on ISO 27001:2013 Implementation.
- STQC – CNSM: Certified Network Security Management
- ISMS Best Practices : ISO/IEC 2700x Awareness and Implementation
- Business Continuity Planning and Disaster Recovery Planning
- STQC-CIISA: Certified Internal Information Security Auditor course

We have rich experience of training more than 10,000 participants from more than 1000 organizations in India and abroad including at Sri-Lanka, China, Dubai, Doha, Mauritius, Singapore

### For details please contact:

**Indian Institute of Quality Management (IIQM), STQC Directorate, Jaipur**

Tel: + 91 141 2756123

Fax: + 91 141 2750464

e-mail: [mbohra@stqc.nic.in](mailto:mbohra@stqc.nic.in)

or

STQC Directorate,

Department of Electronics & Information Technology, Min. of Comm. & IT

New Delhi-110 003

Tel: + 91 11 2436 0219

Fax: + 91 11 24363083

e-mail: [rakesh@deity.gov.in](mailto:rakesh@deity.gov.in)

[www.stqc.gov.in](http://www.stqc.gov.in)