professional training and certification

ISMS Overview

A Program on ISO 27001 Understanding & Implementation

Version 2.1

Government of India
Ministry of Communication & Information Technology
Department of Information Technology
STQC Directorate

ISMS Overview

Objective

- **Understanding of**
  - **Information security – Why? What? How?**
  - **Information Security Management System (ISMS)**
  - **Aspects of ISMS**
  - **Benefits of ISMS**

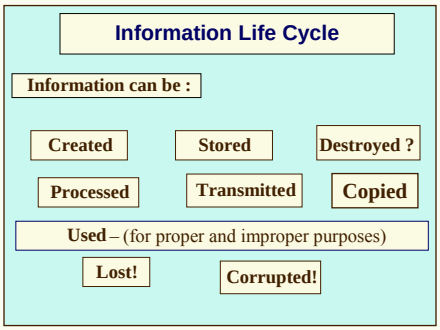
What is Information ?

Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. **(ISO/ IEC 17799)**

Asset: Anything that has value to the organization

Can exist in many forms

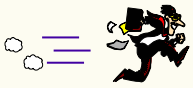
- data stored on computers
- transmitted across networks
- printed out
- written on a paper
- sent by fax
- stored on disks
- held on microfilm
- spoken in conversations over the telephone
- ..



Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected throughout its life cycle

Risk to Information Systems because of

High User knowledge of IT sys.



Theft , Sabotage, Misuse, Hacking

Version Control Problems

Unrestricted Access

Systems / Network Failure

Lack of documentation

Virus

Natural calamities

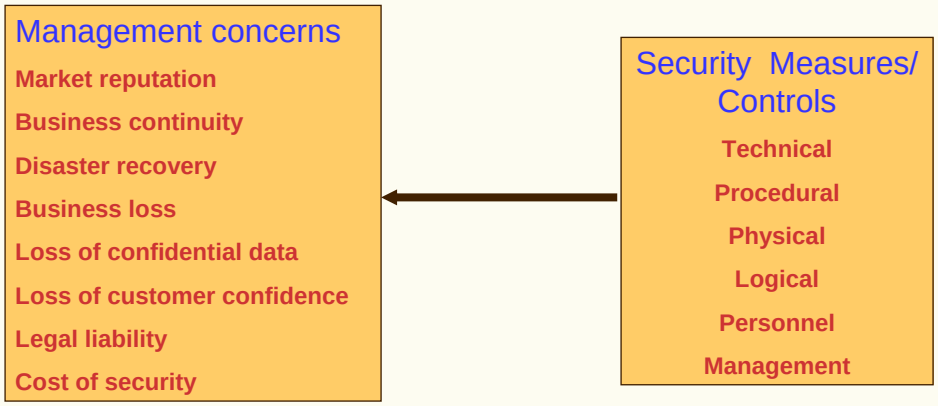
Fire

And the Challenge is…

Protection of Information and Information Systems to meet Business and Legal Requirement by

- Provision and demonstration of secure environment to clients
- Managing security between projects from competing clients
- Preventing loss of product knowledge to external attacks, internal thefts
- Preventing Leak of confidential information to competition
- Meeting Parent company requirements
- Ease of access to large mobile work force
- Providing access to customers where off site development is undertaken with the client.
- Introduction of new technologies and tools
- Managing Legal Compliance
- Managing costs Vs risk

What is needed?

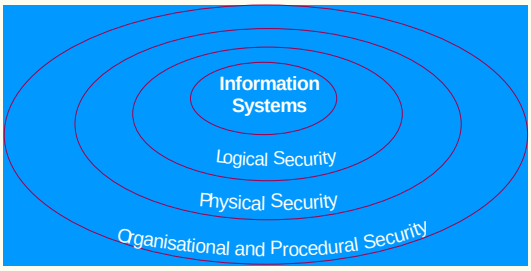


Information Security ……

Information Security is about protecting Information through selection of appropriate Security Controls

- ✓ protects information from a range of threats
- ✓ ensures business continuity
- ✓ minimizes financial loss
- ✓ maximizes return on investments and business opportunities

IS A BUSINESS ISSUE



Objectives of Information Security

Preservation of

Confidentiality :

Ensuring that information is available to only those authorised to have access.

Integrity :

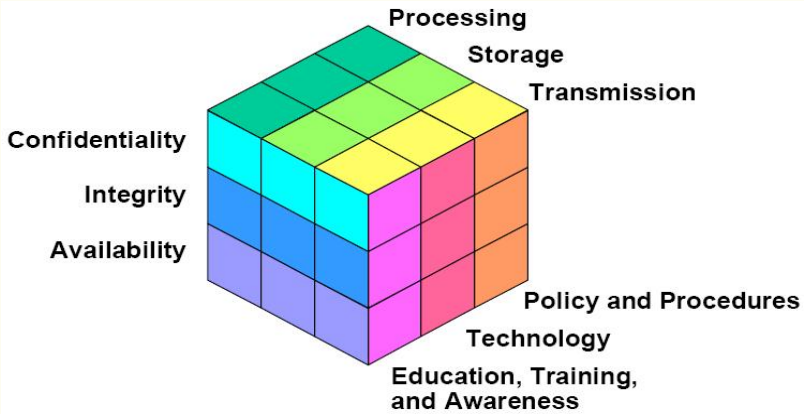
Safeguarding the accuracy and completeness of information & processing methods.

Availability :

Ensuring that information and vital services are available to authorised users when required.

Other practices such as authenticity, accountability, non-reputation and reliability can also be involved.

Information Security Model



But the Problem is….

"To determine how much is too much, so that we can implement appropriate security measures to build adequate confidence and trust"

Why Information Security Management System

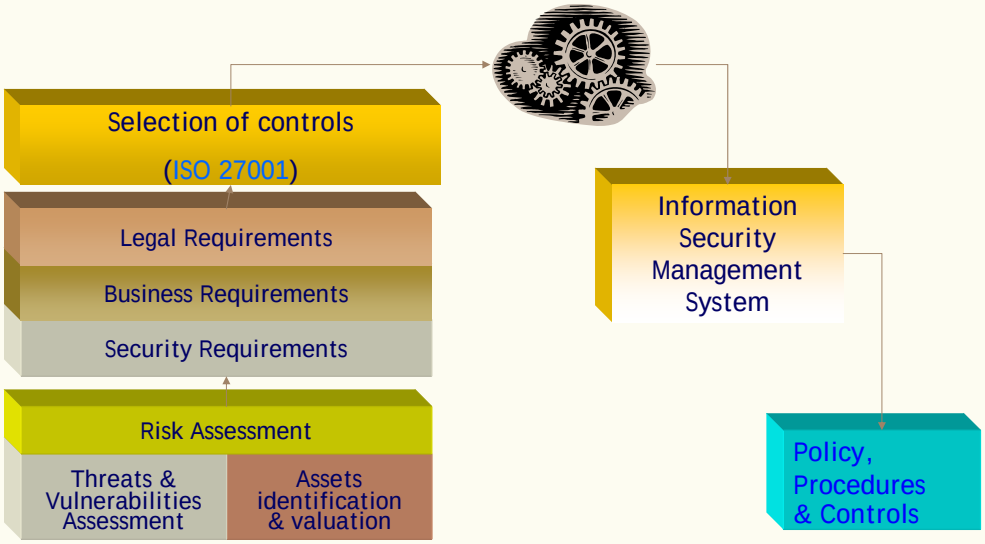
- **Information security that can be achieved through technical means is limited**
- **Security also depends on people, policies, processes and procedures**
- **Resources are not unlimited**
- **It is not a once off exercise, but an ongoing activity**

All these can be addressed effectively and efficiently only by establishing a proper Information Security Management System(ISMS)

Who needs ISMS ?

- Every organization, company, firm institution handling information :
  - **Banks**
  - **Call Centers**
  - **IT Companies**
  - **Government**
  - **Manufacturing Companies**
  - **Consultancy Firms**
  - **Hospitals**
  - **Schools and Universities**
  - **Insurance Companies**
  - **These are examples … Every company which values information and needs to protect it**

Process for developing an ISMS



Information Security Management System

With an ISMS we are not intending to make the system '**hacker proof',** but develop a mechanism which can, to a large extent

- Anticipate potential problems
- Prepare through proactive measures
- Protect against considerable damages
- Ensure recovery and restoration

Benefits of ISMS?

- Assurance through discipline of compliance
- Risk Management
  - Prudent business practice
  - Careful Contracting
  - Use of appropriate controls
- Secure Environment
  - Protection of IPRs.
- Minimized security breaches
  - Continuity of business
- Increased trust & customer confidence & business opportunities

ISMS Standards and ISO 27001 requirements

Objective

- **Understanding of**
  - **ISMS Standards including ISO 27001 and ISO 27002**
  - **ISO 27001 requirements including**
    - Control Objectives and Controls
    - Process Framework Requirements
  - **Future Developments**
- **Benefits of ISO 27001 Implementation**

ISMS Standards -1

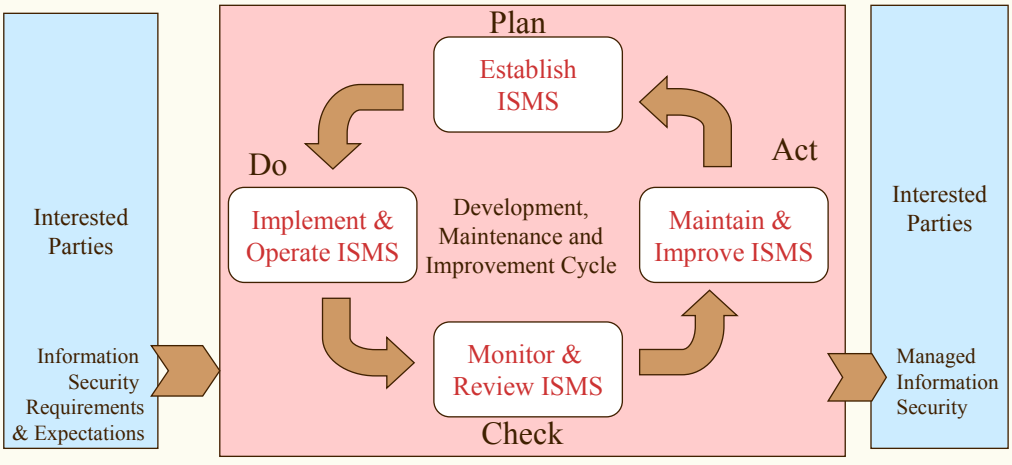
- ISO/IEC 27001: 2005
  - A specification (specifies requirements for implementing, operating, monitoring, reviewing, maintaining & improving a documented ISMS (Within the context of organisation's overall business risks)
  - Specifies the requirements of implementing of Security control, customised to the needs of individual organisation or part thereof.
  - Used as a basis for certification

Both ISO 27001 and ISO 27002 security control clauses are fully harmonized

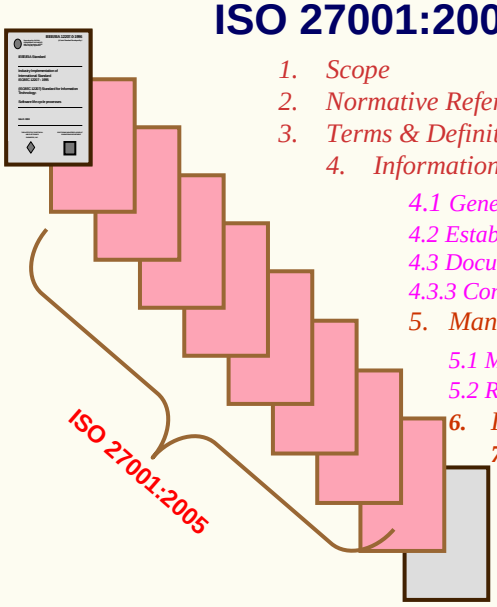
ISMS Standards -2

- ISO/IEC 27002 (earlier ISO/IEC 17799:2005)
  - **A code of practice for Information Security management**
  - **Provides best practice guidance**
  - **Use as required within your business**
  - **Not for certification**

PDCA Model applied to ISMS Processes



ISO 27001:2005 Structure



1. *Scope*
2. *Normative References*
3. *Terms & Definitions*
4. *Information Security Management System*
   - *4.1 General*
   - *4.2 Establish and manage ISMS*
   - *4.3 Documentation*
   - *4.3.3 Control of Records*
5. *Management Responsibility*
   - *5.1 Management Commitment*
   - *5.2 Resource Management*
6. *Internal ISMS Audits*
7. *Management Review of the ISMS*
8. *ISMS Improvement*
   - *8.1 Continual Improvement*
   - *8.2 Corrective Actions*
   - *8.3 Preventive Actions*

*Annexure **A,B & C***

4. Information Security Management System

4. 1 General

4.2 Establishing and managing the ISMS

- **Establish**
- **Implement and Operate**
- **Monitor and Review**
- **Maintain and Improve**

4.3 Documentation requirements

- **4.3.2 Control of documents**
- **4.3.3 Control of records**

5. Management Responsibility

5.1 Management commitment

- ISMS Policy, objectives and plans
- Roles and Responsibilities
- Communication on security objectives, legal and regulatory requirements and continual improvement.
- Adequate resources
- Criteria for accepting risks and the acceptable levels of risk
- Internal ISMS audits
- Management reviews.

5.2 Resource management

5.2.1 Provision of resources for

5.2.2 Training, awareness and competence

6. Internal ISMS Audits

- **Conduct Internal ISMS audits at planned intervals**
- **Documented procedure for Internal ISMS audit**
- **Maintaining records**

Why conduct Internal Audits?
Who conducts Internal Audits?

7. Management Review of the ISMS

7.1 General

- Top management shall review ISMS at planned intervals (at least once a year)

7.2 Review input

7.3 Review output

8. ISMS Improvements

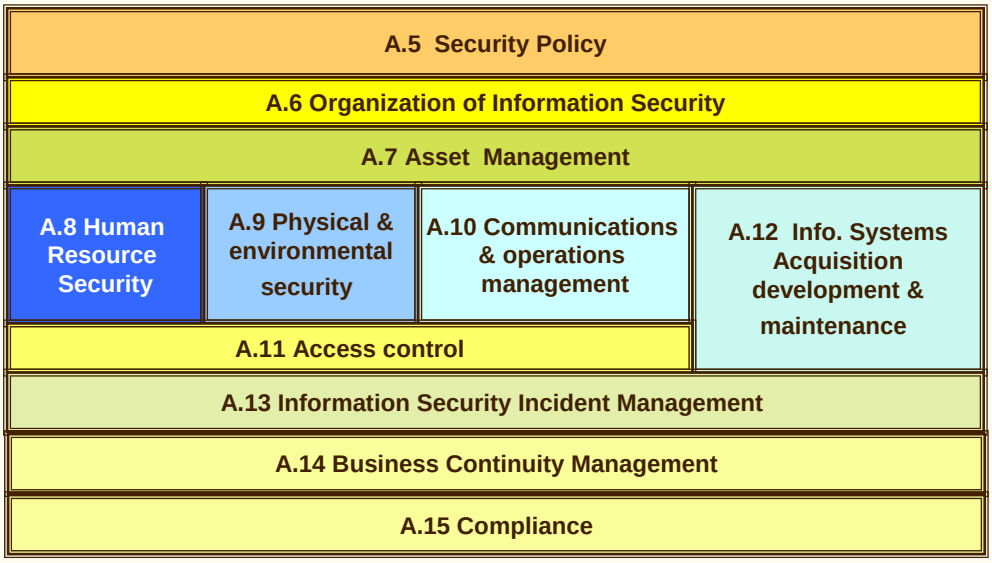
8.1 Continual improvement

8.2 Corrective action

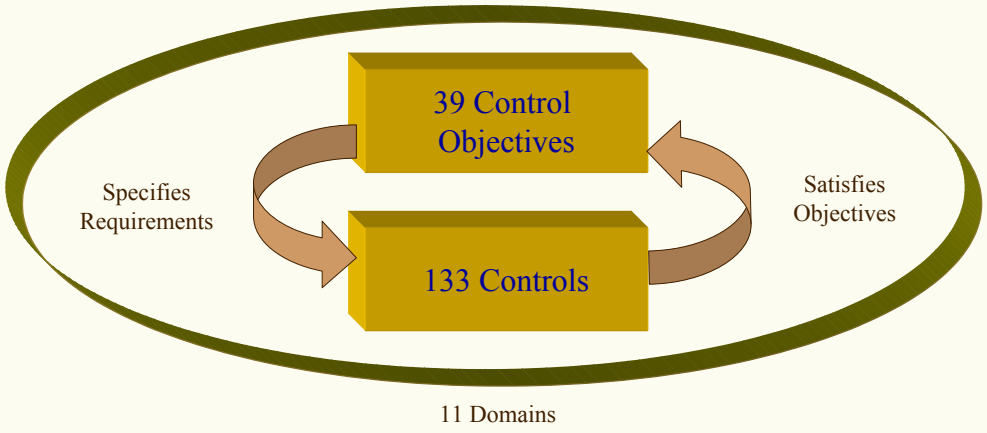
8.3 Preventive action

What is the difference between
Corrective Action and
Preventive action?

Security Domains of ISO 27001



ISO 27001: Control Objectives and Controls



A.5 Organization of Information Security

A.5.1 Information Security Policy

Control Objective : To provide management direction and support for information security.

Controls :

- **Information security policy document**
- **Review of Policy**

A.6 Organization of Information Security

A.6.1 Internal Organization

A.6.2 External Parties

Examples of External parties?

A.7 Asset Management

A.7.1 Responsibility for assets

A.7.2 Information Classification

Top secret	☐
Secret	☐
Confidential	☐
Restricted	☐
Public	☐

A.8 Human Resources Security

A.8.1 Prior to employment

A.8.2 During Employment

A.8.3 Termination or change of employment

COVERS	
Employees	√
Contractors	√
Third Party Users	√

A.9 Physical and Environmental Security

A.9.1 Secure Areas

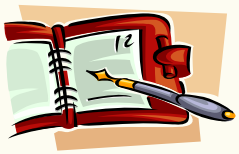
A.9.2 Equipment Security

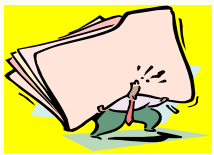
A.10 Communications and Operations Management - 1

A.10.1 Operational Procedures and Responsibilities

A.10.2 Third Party Service delivery management

A.10.3 System Planning and Acceptance





Too much load !

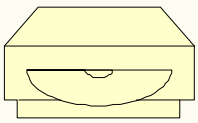
A.10 Communications and Operations Management - 2

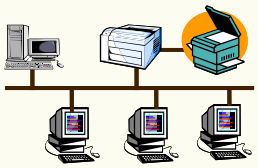
A.10.4 Protection against malicious and mobile code

A.10.5 Back-up

A.10.6 Network Security Management

A.10.7 Media Handling



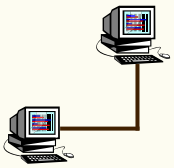


A.10 Communications and Operations Management - 3

A.10.8 Exchange of Information

A.10.9 Electronic commerce services

A.10.10 Monitoring



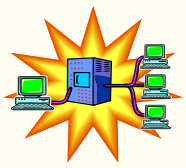
A.11 Access Control - 1

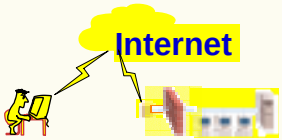
A.11.1 Business Requirement for Access Control

A.11.2 User Access Management

A.11.3 User Responsibilities

A.11.4 Network Access Control



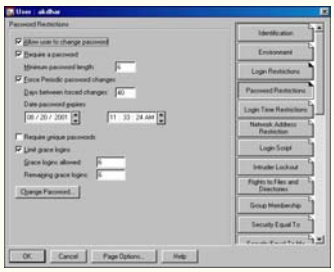


A.11 Access Control - 2

A.11.5 Operating System Access Control

A.11.6 Application and Information Access Control

A.11.7 Mobile Computing and Teleworking



A.12 Information Systems Acquisitions, Development and Maintenance

A.12.1 Security Requirements of Info. Systems

A.12.2 Correct processing in applications

A.12.3 Cryptographic controls

A.12.4 Security of system files

A.12.5 Security in dev. and support processes

A.12.6 Technical vulnerability management

A.13 Information Security Incident Management

A.13.1 Reporting info. security events and weaknesses

A.13.2 Management of info. Security incidents & improvements

A.14 Business Continuity Management

A.14.1 Information Security Aspects of BCM

Control Objective : To counteract interruptions to business activities and to protect critical business processes from the effect of major failure or disasters and to ensure their timely resumption.

Controls :

- **Including info. security in the BCM management process**
- **Business continuity and risk assessment**
- **Developing and implementing continuity plans including Information security**
- **Business continuity planning framework**
- **Testing, maintaining and re-assessing business continuity plans**

Difference between incident and disaster ?

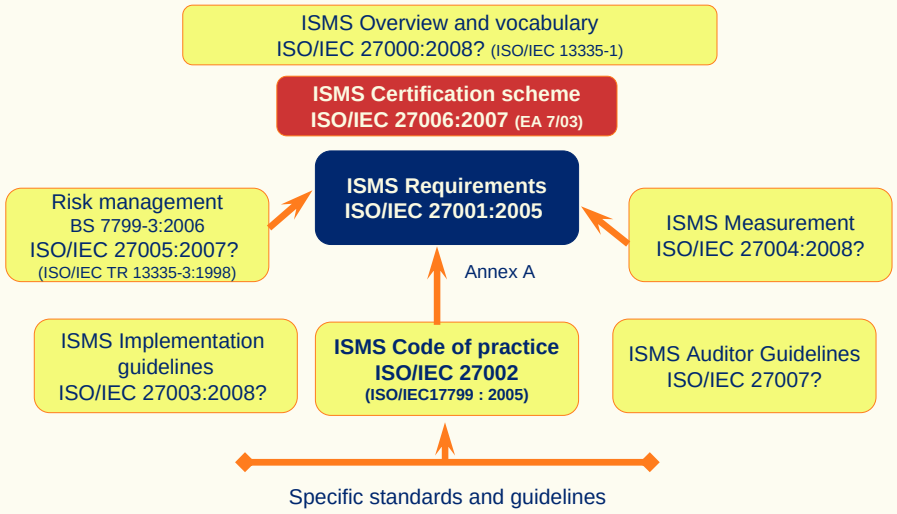
A.15 Compliance

A.15.1 Compliance with Legal Requirements

A.15.2 Compliance with security policies and standards, and technical Compliance

A.15.3 Information systems audit considerations

ISO/IEC 27000 family review including future development



Benefits of ISO 27001

- A single reference point for identifying a range of controls needed for most situations where information systems are used
- Facilitation of Trading in trusted environment
- An internationally recognized structured methodology
- A defined process to evaluate, implement, maintain and manage information security
- A set of tailored policy, standards, procedures and guidelines
- The standard provides a yardstick against which security can be judged

ISMS Implementation

Action Plan for ISMS Implementation

- Project Initiation
- **Formation of Security organization including CISO**
- Identify roles and responsibilities of groups
- Management intent on ISO 27001 initiative communicated to all
- Framing and Approval of Scope and Security Policy Statement
- Communication to all
- **Risk Analysis/Assessment**
  - Methodology of RA
  - Asset Identification
  - Training on RA
  - Actual RA
  - Asset classification guideline (Labeling/Handling)
  - Risk Treatment Plan & Actual implementation
- Preparation of SOA

Action Plan for ISMS Implementation-2

- ***Gap Analysis / Status Appraisal*** (May also be done before RA)
- Vulnerability assessment, Application Security Testing (May also be done before RA)
- Documentation of Policies and Procedures
- Identification and documentation of Legal requirements and Business Requirements
- Security Awareness training
- Implementation of Policies and Procedures
- Business Continuity Planning
  - Carrying out BIA
  - Writing BCP
  - BCP Organisation
  - Training
  - BCP Testing and Updation

Action Plan for ISMS Implementation-3

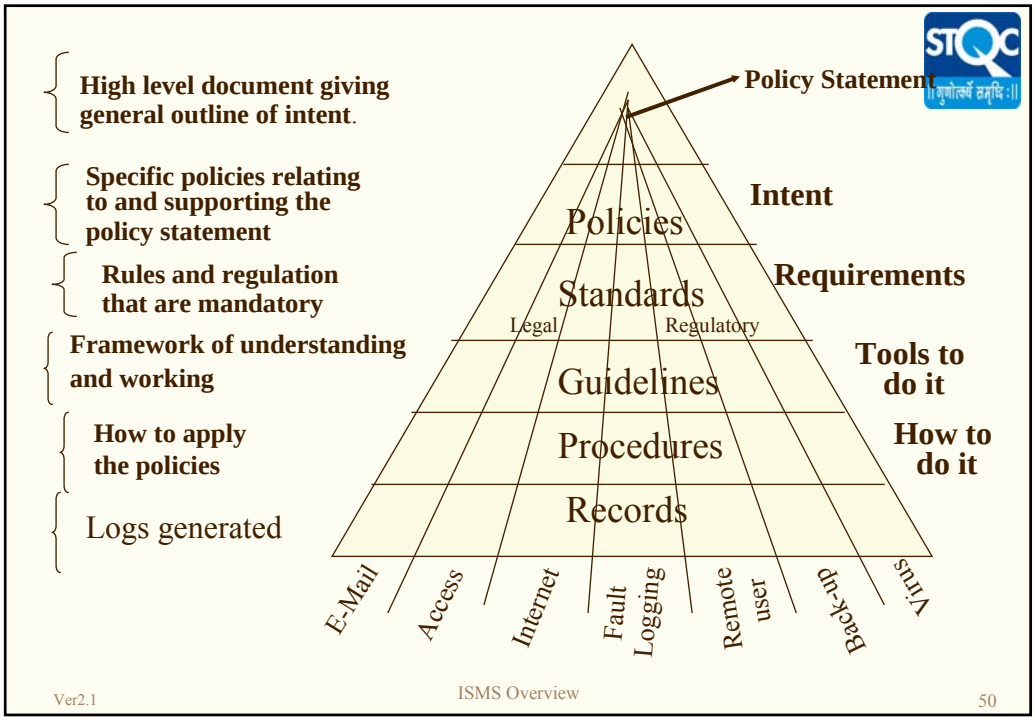
- Monitor and Review ISMS effectiveness
  - Internal ISMS Audits
  - Management Reviews
- Improve ISMS
- Apply for Certification

ISMS Documentation

ISO 27001 para 4.3.1

- **Documented statements of ISMS policy including information security policies and security objectives.**
- **Scope of ISMS**
- **Procedures and controls in support of the ISMS**
- **Risk Assessment methodology**
- **Risk Assessment Report**
- **Risk Treatment Plan**
- **documented procedures needed to ensure effective planning, operation and control of information security processes. Including KPIs e.g**
  - **Incident management**
  - **Business Continuity Planning**
  - **Change Control Procedure**
- **Records**
- **Statement of Applicability**

Documents and records can be in any form or type of medium



Example : Policies required

- **Information security**
- **Clear Desk and Clear Screen**
- **E-mail security**
- **Information exchange.Thru fax, voice**
- **Access Control**
- **Mobile computing /Teleworking**
- **Cryptographic Control**
- **Anti- Virus Policy**
- **Password Policy**
- **Change management**

OBJ

Procedures Required

- Documented Procedures Required in the mandatory section of ISO 27001
  - Control of Documents
  - Control of Records
  - Internal ISMS Audits
  - Corrective Actions
  - Preventive Actions
  - Risk Assessment Procedure
- Documented Procedures Required to support selected Controls
  - Operating Procedures identified in Security Policy

Examples follow:

Example: Procedures Required by Organization

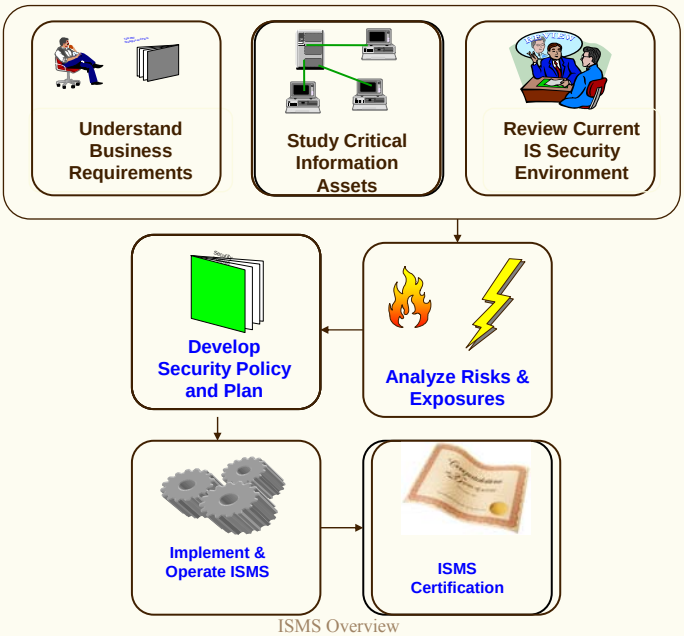
- Acceptable use of Assets
- Information labeling & Handling
- Roles and Responsibilities
- Disciplinary Process
- Migration of software
- Acceptance criteria for new info. Sys.
- Control against Malicious s/w
- Handling & storage of info
- Monitoring of Use of Info. System
- Access Control Policy
- User Reg. & de-Reg.
- Allocation of Passwords
- Review of User access rights
- Key management system
- Control of operational software
- Software Change control
- Incident Management including reporting
- Identification of appl. Legislation

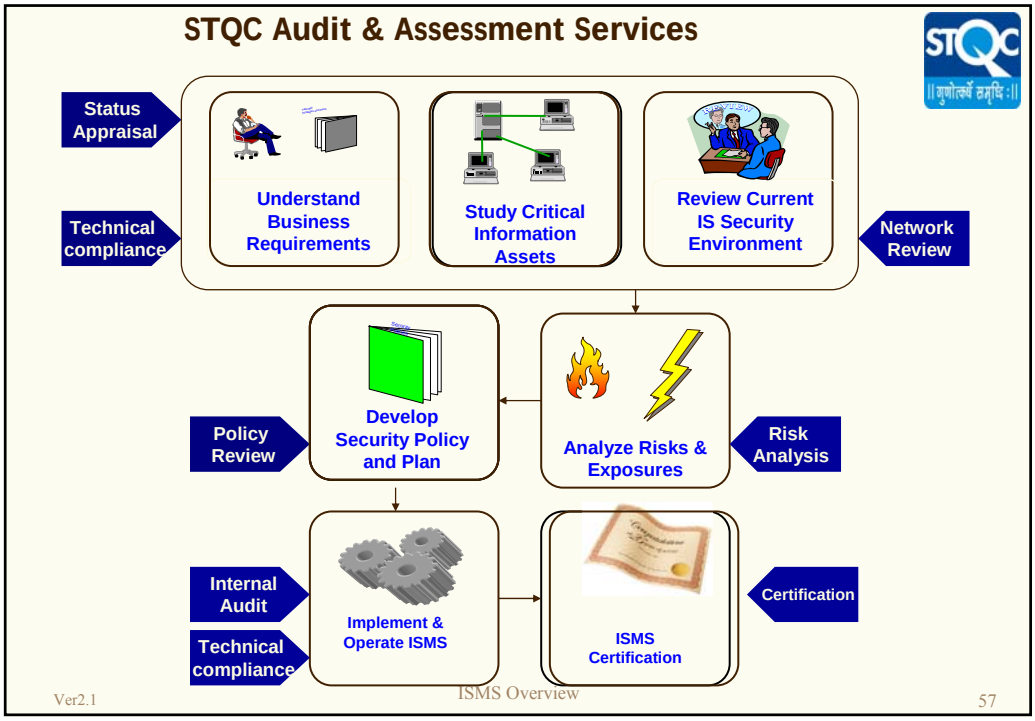
Benefits of Implementation

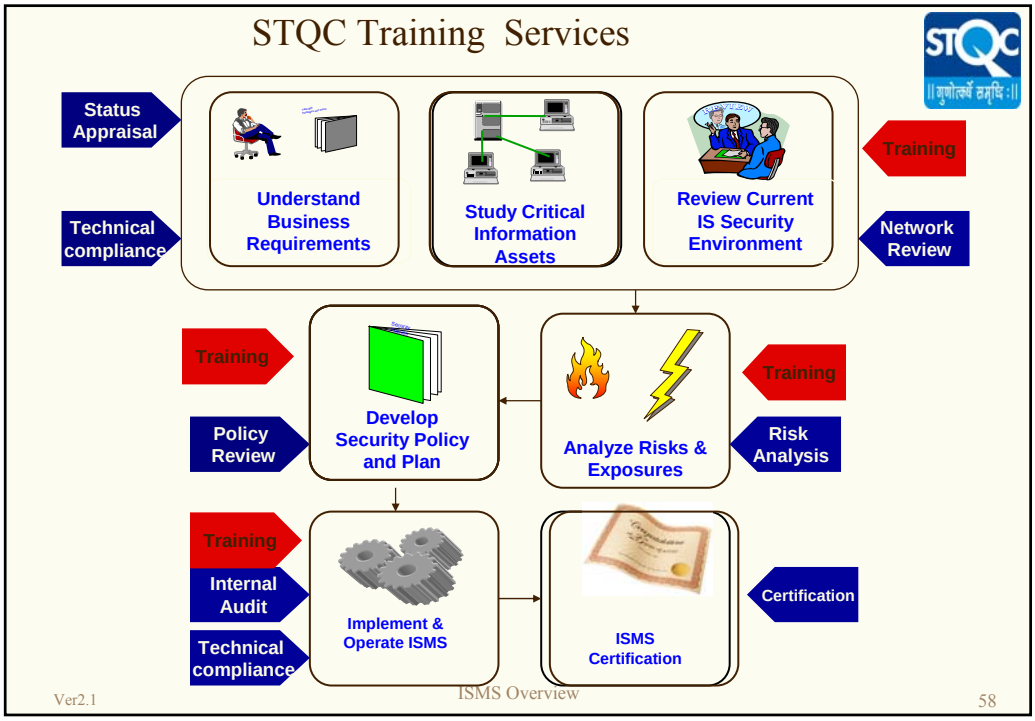
- Enhances knowledge and importance of security related issues at the management level.
- Improves understanding of business aspects
- Reductions in security breaches and/ or claims
- Reductions in adverse publicity
- Improves insurance liability rating
- Identifies critical assets via the Business Risk Assessment
- Provides a structure for continuous improvement
- Enhances Information Security factor internally as well as externally

STQC's Role in ISMS

ISMS Implementation Steps




STQC Audit & Assessment Services
Status Appraisal
Technical compliance
Understand Business Requirements
Study Critical Information Assets
Review Current IS Security Environment
Network Review
Develop Security Policy and Plan
Policy Review
Analyze Risks & Exposures
Risk Analysis
Internal Audit
Technical compliance
Implement & Operate ISMS
ISMS Certification
Certification
Ver2.1
ISMS Overview
57


STQC Training Services
Status Appraisal
Technical compliance
Understand Business Requirements
Study Critical Information Assets
Review Current IS Security Environment
Training
Network Review
Training
Develop Security Policy and Plan
Policy Review
Analyze Risks & Exposures
Training
Risk Analysis
Training
Internal Audit
Technical compliance
Implement & Operate ISMS
ISMS Certification
Certification
Ver2.1
ISMS Overview
58

STQC's Role in Information Security

- **Playing Catalytic Role for promotion of ISMS in India.**
  - **First Certification Body for BS7799/ ISO 27001 Standard in India. There are at present 9 certification Bodies.**
  - **Internationally recognized Training Organisation for CEH Programs, ISMS LA, itSM LA and Consultant Programs.**
  - **Other programs include on ISMS implementation (STQC-CISP), Internal Auditing (STQC-CIISA), BCP, Risk Assessment etc.**
- **STQC is a third party assurance organization under the NeGP Project of GOI, assuring compliance to Quality, Security and Service parameters.**
- **Participation in BIS Meetings for adaptation and adoption of standards as IS Standards.**

STQC's Role in Information Security

- **STQC is registered as member to the Common Criteria Recognition Arrangement (CCRA) with other 24 countries as certificate consuming country**
- **CC lab is established**
- **STQC has taken pilot projects to become certificate producing country**
  - **SCOSTA OS for National ID cards**
  - **Intrusion Detection System**
- **STQC can provide Trainings in CC area.**

Thankyou.

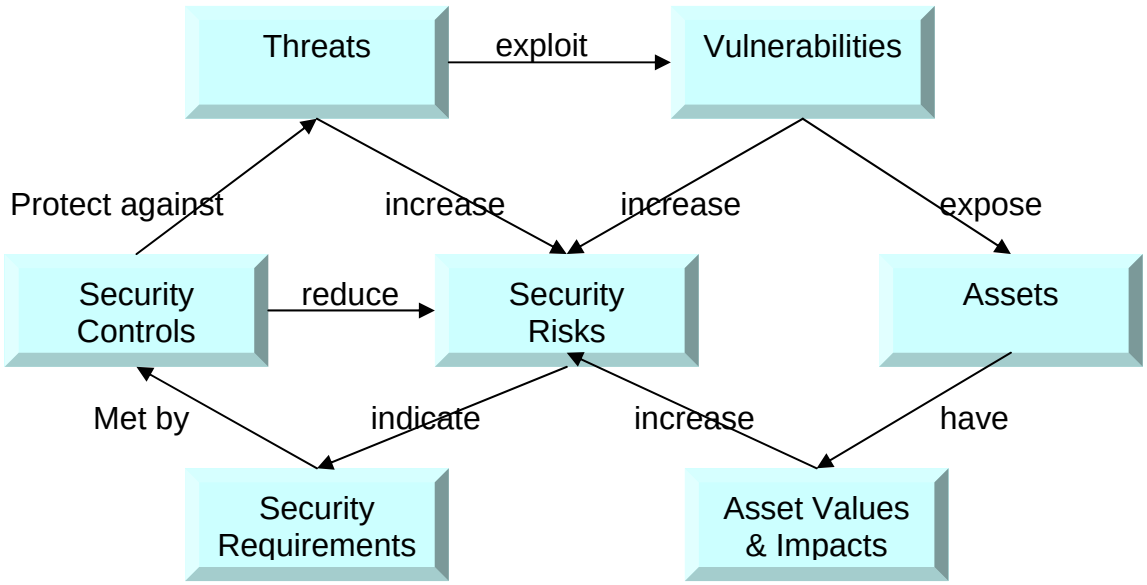
For more information please contact

Arvind Kumar
arvind@mit.gov.in

Rakesh maheshwari
rakesh@mit.gov.in

ISMS Auditor / Lead Auditor Training Course

An IRCA Approved Training Course
by
Indian Institute of Quality Management (IIQM)
(Course Approval Number A17226)
(TO Approval Number AO17225)



Indian Institute of Quality Management
STQC Directorate
Department of Information Technology
Ministry of Communication & Information Technology

About ISMS Auditor / Lead Auditor Training Course

This training course is designed for those who wish to become Information Security Management System (ISMS) auditor and is based on ISO 27001:2005

Successful qualification in Auditor / Lead Auditor training course is a pre-requisite for IRCA empanelment of ISMS Auditors.

This training course is an IRCA (International Register of Certificated Auditors) approved training course for Auditors / Lead Auditors. (Approval Number A17226)

Course Objectives

To gain knowledge & skill for conducting ISMS audits.

Knowledge:

- Understand the purpose of ISMS and the processes involved in establishing, implementing, operating, monitoring, reviewing, maintaining and improving an ISMS as defined in ISO 27001: 2005.
- Understand the purpose, content and interrelationship of ISO 27001: 2005, ISO/IEC 17799 and ISO 19011, ISO/IEC TR 13555 Parts 3 and 4 (GMITS), EA 7/03 and the legislative framework relevant to ISMS.
- Understand the role of an auditor to plan, conduct, report and follow up an ISMS audit in accordance with ISO 19011.

Skill:

- Interpret the requirements of ISO 27001: 2005 and EA 7/03 in the context of an ISMS audit.
- Undertake the role of an auditor to plan, conduct, report and follow up an audit in accordance with ISO 19011.

Course Contents

The program is Highly Skill Oriented and is based on Accelerated Learning Techniques recommended by IRCA. Following main topics suitably supported with a number of Exercises (Individual as well Team Exercises) are covered.

• ISMS concepts & benefits	• ISMS standards
• Risk assessment & Risk management	• Business continuity management
• Incident management	• Audit fundamentals
• Audit management standard	• Audit planning
• Audit execution	• Audit reporting
• Audit follow-up	• ISMS certification process
• IRCA empanelment & code of conduct	• Examination

Who Should Attend

This training course is meant for those who wish to become ISMS Auditor. These may be

Information security practitioners
Information security officers / Managers
ISMS Designers
ISMS Consultants
System Managers / Administrators

Pre-requisites

It is expected that participants have completed University level of education. Participants should be working professionals and are also expected to have an understanding of the principles supporting ISMS and of the ISO 27001: 2005 standard.
The course focuses on teaching & developing ISMS audit skills and should not be looked as basis for learning ISMS.

Assessment and Examination

The training course has built in continuous assessment and a written examination on 5th day afternoon at the conclusion of the course. Successful qualification in both is essential to qualify for Auditor / Lead Auditor certificate. Successful participants will be awarded IIQM, STQC certificate with IRCA logo on it. Other participants shall get participation certificate from IIQM, STQC.

Course Duration and Timings

The course duration is Five Days.
The training course will be held 0830 hrs to 1845 hrs daily except on 5th day, when it will be over at 1730 hrs

Course Material

The delegates will receive standards (IS/ISO 17799, ISO 27001 & IS/ISO 19011) for use during the course and course material consisting of

- Participants material
- Exercise manual
- Stationery

Course Fee: The course is delivered as a public programme as well as can be conducted on-site either at STQC premises or at client premises. For detailed fee in each of these category please contact IIQM / STQC.

Other details

Each course will have **maximum of 20 participants**.

Medium of course delivery shall be **English**.

The ISMS Auditor/ Lead auditor programs are conducted at STQC Centers. Corporate programs can also conducted ON SITE.

Other relevant training programs conducted by STQC IT Services / IIQM are

Courses conducted by STQC IT Services	Courses conducted by IIQM
STQC-CISP (STQC Certified Information Security Professional) – 5 days STQC-CIISA (STQC Certified Internal Information Security Auditor) – 3 days STQC- CEHP (STQC Certified Ethical Hacking Professional Course) – 5 days ISO 20000 Auditor Program for ITSM (itSMF Accredited) - 2 days Certified Software Quality Professional (CSQP) – 5 days Certified Software Test Manager (CSTM) – 3 days	ISO 9000: 2000 Series Auditor / Lead Auditor Training Course ISO 9000: 2000 Series Foundation and Internal QMS Auditor Training Course Laboratory Quality Management System and Internal Audit as per ISO 17025:2005 and ISO 15189 M.S. Quality Management (BITS Pilani / IIQM collaborative program).

STQC DIRECTORATE
Department of Information Technology,
Ministry of Comm. and IT,
GOVT. OF INDIA

STQC Certified Information Security Professional (STQC-CISP)

This STQC-CISP training course is designed for individuals and organizations planning to implement Information Security Management System (ISMS). The course provides Knowledge and Skills for ISMS Implementation based on ISO/IEC 27001: 2005 and ISO/IEC 17799:2005, the internationally acknowledged standards for Information Security.

On successful qualification of STQC-CISP course, the professional will be able to understand ISMS processes and implementation of ISO/IEC 27001:2005 standard.

Course Objectives

- To learn the purpose of an Information Security Management System (ISMS) and the processes involved in establishing, implementing, operating, monitoring, reviewing and improving an ISMS as defined in ISO 27001: 2005
- To develop necessary framework for effective implementation of ISMS
- To understand Business Continuity management and develop BCP
- To understand the requirements for Legal compliance for an effective ISMS.
- To understand and implement the security controls of ISO 27001: 2005

Course Contents

The course is focused to gain in depth knowledge of ISMS process and interpretation of requirements as per ISO 27001: 2005. Following main topics suitably supported with a number of Exercises (Individual as well Team Exercises) are covered.

• Role of Information Security Management System (ISMS) in business • ISMS Implementation Overview • ISMS Implementation issues related to defining Scope & Security Policy • Risk Assessment Concepts and Approaches • Preparing a Statement of Applicability (SoA) • ISO27001 Security Controls	• ISMS Documentation • Security Policy Writing • Business Continuity Management • Legal/Contractual Compliance • ISMS Training and Awareness • Review and Audit of ISMS • ISMS Certification

Who Should Attend

This training course is meant for those who wish to learn the implementation of ISMS as per requirements contained in ISO 27001: 2005 and best Practices contained in ISO 17799:2005 standard. These may be

- Persons responsible for the implementation of ISMS
- ISMS/ QMS Consultants
- Information Security Officers

- ISMS/ QMS Auditors (Internal or External)
- ISMS Designers
- System Managers / Administrators

Course Pre-requisites

It is expected that participants have completed University level of education. Participants should be working professionals and are also expected to have an understanding of the principles supporting ISMS and of the ISO 27001: 2005 standard. Audit Experience will be an added advantage.

Assessment and Examination

The training course has built in continuous assessment and a written examination on 5th day afternoon at the conclusion of the course. Successful qualification in both is essential to qualify for STQC-CISP certificate. Participants achieving a score of 70% and above will be awarded the **Certified Information Security Professional (STQC-CISP).** Others will get a certificate of Attendance.

Course Duration and Timings

The course duration is five days. The course will be held during 0930 hrs to 1730 hrs daily except on 5th day, when it will be over at 1500 hrs

Course Material

The delegates will receive a standard course book prepared by STQC along with useful documents including exercise manual etc during the commencement of course. Relevant Standards will be provided for use during the course.

Other details

The STQC-CISP courses are conducted at STQC Centers. For details of venue and dates, please visit STQC website or contact STQC Directorate, New Delhi / nearest STQC IT Center.

Medium of course delivery shall be English.

STQC DIRECTORATE
Department of Information Technology,
Ministry of Comm. and IT,
GOVT. OF INDIA

STQC Certified Internal Information Security Auditor (STQC-CIISA)

The STQC-CIISA training course is designed for individuals and organizations interesting in learning the means of determining the effectiveness of ISMS in an organization through internal audits of Information Security Management System (ISMS). The course provides comprehensive knowledge and skills for conducting the internal of ISMS Implementation and measuring its effectiveness based on ISO/IEC 27001: 2005 and ISO/IEC 17799:2005, the internationally acknowledged standards for Information Security.

On successful qualification of STQC-CIISA course, the professionals will be able to understand ISMS processes, auditing skills and determining the effectiveness of the ISMS.

Course Objectives

- To learn the various techniques of an internal audit
- To understand security controls of ISO 27001: 2005 standard
- To Know how to conduct Internal ISMS audits based on ISO27001 requirements
- To qualify as Certified Internal Information Security Auditor (STQC-CIISA)

Course Contents

The course is focused to acquire good understanding of ISMS process and learning the auditing skills for ISMS as per requirements as per ISO 27001: 2005. Following main topics suitably supported with a number of Exercises (Individual as well Team Exercises) are covered during the course.

• ISMS Framework and recap of ISO27001 • Role of audit in Information Security Management System (ISMS) • Concepts and principles of Auditing based on ISO 19011 • ISMS Audit life cycle processes • ISMS Audit planning	• ISMS Audit execution including auditing techniques • ISMS Audit reporting –Positive/ non-conformance reporting, Classification of NCs, and measuring effectiveness of ISMS • Exercises and Case Studies

Who Should Attend

This training course is meant for those who wish to learn ISMS security controls and internal auditing of the ISMS as ISO 27001: 2005. These may be

- Chief Information Officers
- IT Managers
- System /Network Managers or Administrators
- Persons responsible for the implementation and management of ISMS

- ISMS/ QMS Consultants
- Existing Auditors (QMS /EMS/ Finance/Safety etc.)
- Security forum Members

Course Pre-requisites

It is expected that participants have completed University level of education. Working professionals having prior awareness and knowledge ISO 27001: 2005 and or ISO/IEC 17799:2005 standard will be an added advantage.

Assessment and Examination

The training course has built in continuous assessment and a written examination on 3rd day afternoon at the conclusion of the course. Successful qualification in both is essential to qualify for STQC-CIISA certificate. Participants achieving a score of 70% and above will be awarded the **Certified Internal Information Security Auditor (STQC-CIISA).** Others will get a certificate of Attendance.

Course Duration and Timings

The course duration is three days. The course will be held during 0930 hrs to 1730 hrs daily.

Course Material

The delegates will receive a standard course book prepared by STQC along with useful documents including exercise manual etc during the commencement of course. Relevant Standards will be provided for use during the course.

Follow up Courses :

- ISMS Lead Auditor Course
- STQC Certified ISMS Professional (STQC-CISP)

Other details

The STQC-CIISA courses are conducted at STQC Centers. For details of venue and dates, please visit STQC website or contact STQC Directorate, New Delhi / Indian Institute of Quality Management, Jaipur.

Medium of course delivery shall be English.

STQC DIRECTORATE
Department of Information Technology,
Ministry of Comm. and IT,
GOVT. OF INDIA

STQC Certified Ethical Hacking Professional (STQC-CEHP)

Course Description :

With the growth of the Internet, information security has become a major concern for businesses and governments. They want to be able to take advantage of the Internet for electronic commerce, advertising, information distribution and access, and other pursuits, but they are worried about the possibility of being "hacked." At the same time, the potential customers of these services are worried about maintaining control of personal information that varies from credit card numbers to social security numbers and home addresses.

To tackle this complex problem of intrusion and hacking the conventional methods like deployment of various technological and managerial controls may not be effective if one is unable to pinpoint the weaknesses of his system. One of the best ways to identify the system weaknesses is to have independent information security professionals attempt to break into their computer systems. This is similar to having independent auditors come into an organization to verify its financial or other management systems. In the case of information security, "ethical hackers" would employ the same tools and techniques as the hackers, but they would neither damage the target systems nor steal information. Instead, they would evaluate the target systems' security and report the discovered vulnerabilities with recommendations to plug it with suitable countermeasures.

The STQC-CEHP Program certifies individuals to conduct Ethical Hacking. This program will also benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the security of the network infrastructure. The course is designed to introduce, how hacking skills can be used for the defense of IT infrastructure without harming the infrastructure, through interactive theoretical and practical sessions.

Who should attend :

- Network Administrator
- Network Security Auditors
- Network security Consultant

Prerequisites :

- Computer Networking and TCP/IP
- Knowledge on Windows NT/2000 Server Administration
- Knowledge on security components like firewall, IDS etc.

Course Content :

Module 1: Overview of E-Security and Ethical Hacking

- Importance of security
- Introducing ethical hacking and essential terminologies
- Understanding different phases of hacking
- E-security testing

Module 2: Common E-Security Threats and Vulnerabilities

- Passive Threats
- Active Threats
- DoS
- Buffer Overflow
- Top 20 Internet Vulnerabilities
- Vulnerability Database(ICAT etc.)

Module 3: Linux and Security

- Installation of Linux OS
- Installation of applications
- Essential Linux commands
- Configuring TCP/IP Network
- Configuring and Launching different services
- Essential Linux tools and utilities
- VA and Hardening of Linux

Module 4: Network and E-security Devices

- Hub, Switch and Router
- Working principle
- Security Issues
- Firewall
    - Concepts
    - Types of Firewall
    - Demo
- IDS
    - Concepts
    - Types of IDS
    - Demo
- Honey Pots
    - Concepts
    - Demo
- Evading Firewall and IDS
    - Techniques
    - Demo

Module 5: Reconnaissance

- Discover initial information
- Locate the network/IP range
- Know the active machines in the target Network
- Estimate the network configuration
- Mapping the Network
- Tools

Module 6: Scanning

- Port Scanning
- Active and passive fingerprinting
- Discovering running services
- Vulnerability scanning
- War dialing
- Vulnerability Scanning
- Tools

Module 7: Enumeration

- Concepts
- NetBIOS Null Session
- NetBIOS Enumeration
- SNMP Enumeration
- Tools
- Countermeasures

Module 8: System Hacking

- Password cracking
- Privilege escalation
- Keystroke loggers
- Root-kits
- Covering tracks
- Hiding files
- Steganography
- Tools
- Countermeasures

Module 9: Sniffing

- Overview of Sniffers
- Active and Passive Sniffing
- ARP Spoofing and Redirection
- DNS Spoofing
- Tools
- Countermeasures

Module 10:Virus Trojans and Back doors

- Defining Virus
- Types of Virus
- Defining Trojans and backdoors
- Some popular trojans
- Trojan creation
- Wrappers

- Anti-Trojan software
- Trojan detection and removal techniques

Module 11: Web server and web application vulnerabilities

- Introduction to Web Servers
- Popular Web Servers and common Vulnerabilities
  - Apache Web Server Security
  - IIS Server Security
- Web Application Authentication
  - HTTP Authentication Basic & Digest
  - NTLM Authentication
  - Certificate Based Authentication
  - Forms Based Authentication
- Common Web Application Security Vulnerabilities
- Web Application Penetration Methodologies
  - Input Manipulation
  - Cross site scripting
  - Password cracking
  - SQL injection

Module 12: E-security through Encryption

- Symmetric and Asymmetric Key encryption
- Message Digest
- Digital Signature
- Certificate Authority(CA)
- IPSec

Module 13:WLAN Security

- Introduction to Wireless LAN and 802.11
- Finding WLANs
- WEP and its weakness?
- Wireless DoS attacks
- WLAN Scanners
- WLAN Sniffers
- Securing Wireless Networks
- Tools
- Countermeasures

Course Duration :

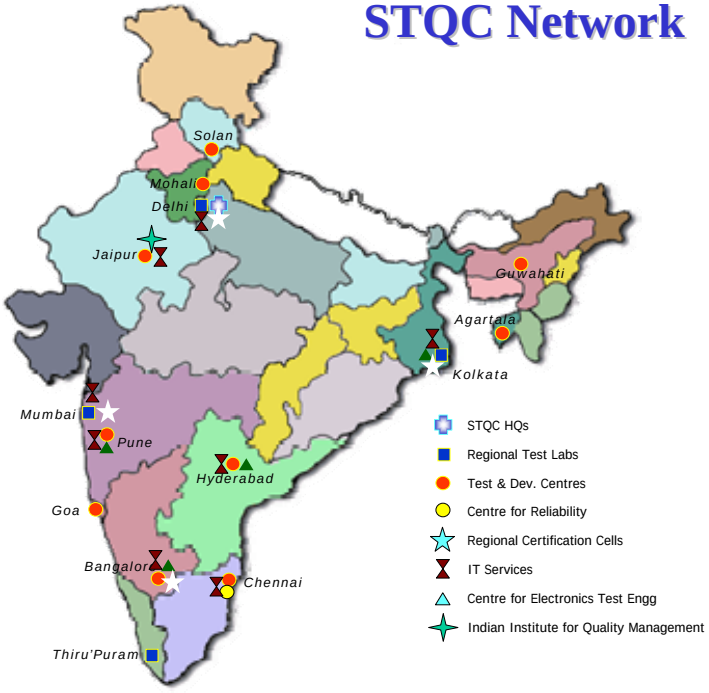
5 days +1 day

One day is required for ensuring proper preparation of lab infrastructure .

Follow up Courses:

- Certified Information Security Professional (STQC-CISP)
- Certified Internal Information Security Auditor (STQC-STQC-CIISA)

STQC Network



STQC IT Services