Global Standards in Information Security Management and STQC experience in their implementation and auditing

Rakesh Maheshwari
STQC Directorate,
Department of Information Technology,
Min. of Comm. and IT
rakesh@mit.gov.in

Broad Contents

- About STQC IT
- ISMS Services
- ISMS Certification
- ISMS implementation
- Issues
- Improvements seen as a results of ISMS compliance
- Conclusion

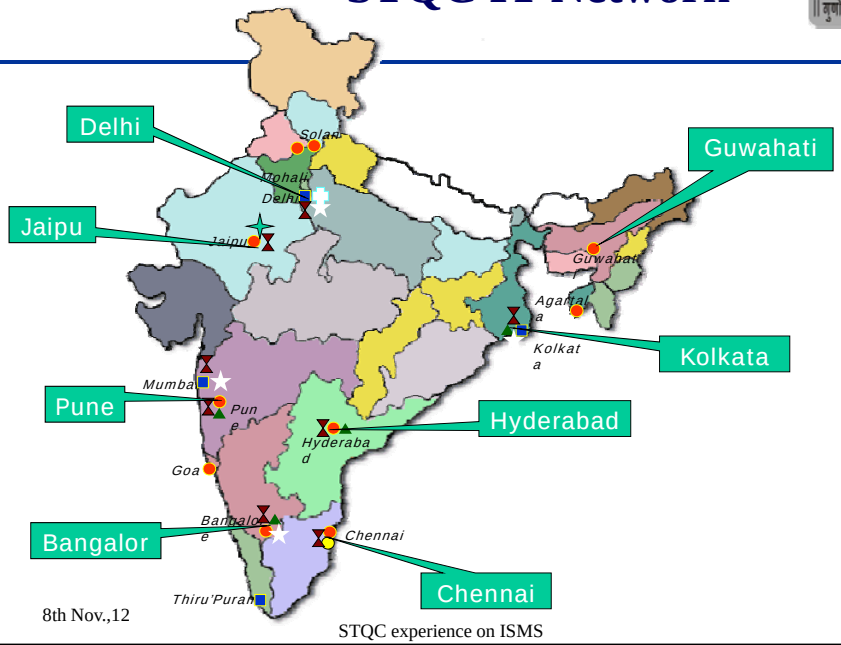
Standardisation Testing & Quality Certification Directorate

Standardisation
Testing
Quality
Certification

An attached office of DeitY

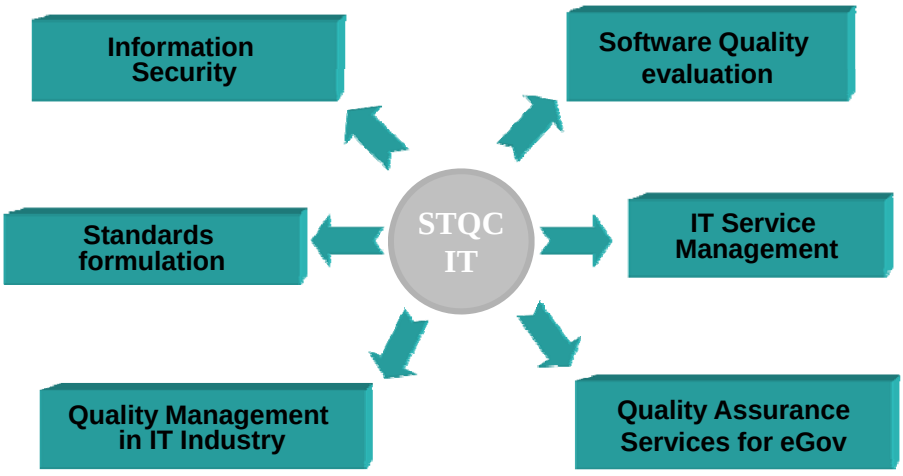
8th Nov.,12 3

STQC IT Network



8th Nov.,12 STQC experience on ISMS 6

STQC Services for IT Sector



8th Nov.,12 STQC experience on ISMS 7

Information Security Management Services

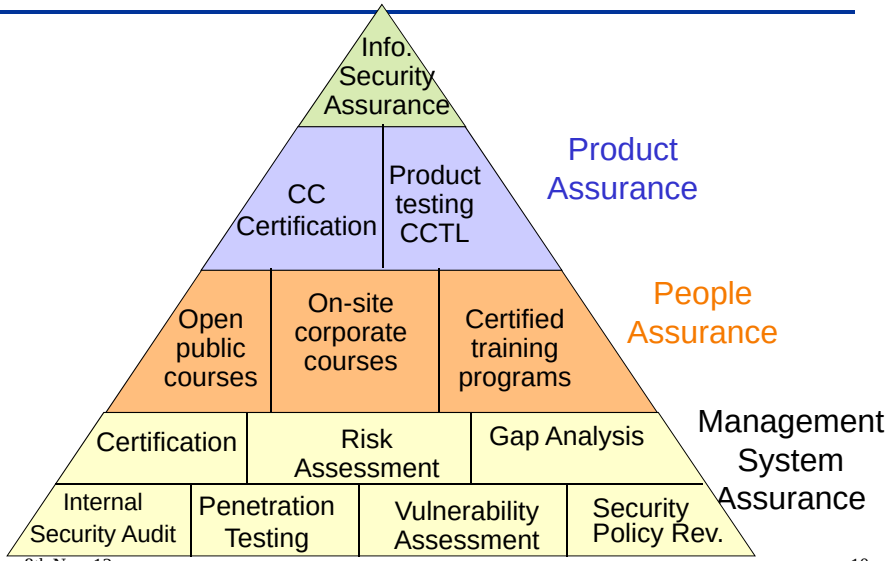
Information Security

- **Information Security Management System Certification (ISMS) based on ISO 27001**
- **Audit and Review service to industry in establishing secure networks and information system through :**
  - **Penetration Testing**
  - **Vulnerability Analysis**
  - **Application security**
  - **RISK assessment**
  - **Business Continuity and Disaster Recovery planning**
- **Listed with CERT-IN**
- **Internationally accredited training programmes like ISMS Lead assessor and certified Information Security Professional**
- **Technical co-operation with NIST-USA under Indo-US Cyber Security Programme**
- **Common Criteria Test Lab and Certification Scheme (ISO 15408)**

STQC is the FIRST CB accredited by RvA, Netherlands as per ISO 27006: 2007/ 17021:2006

8th Nov.,12 9

Information security assurance framework



8th Nov.,12 STQC experience on ISMS 10

ISMS Certification

Information Security Certification – Client profile

Certified more than 50 organizations in different sectors

- Software development	- Banks	- Project Management
- Manufacturing	- BPOs	- Component Design
- Data Centres	- Pharmaceuticals	- Automobiles
- Telecom	- Government	

Overseas services provided in
- China - Mauritius - Taiwan
- UAE - Qatar - USA

STQC is the first organization outside Europe to get international accreditation to provide certification as per ISO 27001 standards

ISMS Certification- status

- ISO 27001 accepted as defacto **Baseline security standard.**
- India is among One of the first few Countries who initiated ISMS Certifications after UK and Netherlands
- **More than 600 certified organisations** have been certified. Majority of them from SW development , BPO, Data center, Automobiles, Telecom, Pharmaceuticals etc. **India stands Third in the World tally of ISO27001 certifications**
- A large **work force of Security Professionals** CISA, CISSP, BS 7799/ ISO 27001 Lead assessors
- Active ISMS Certification Bodies in India - DNV, BSI , KPMG , BVQI,TUV, CIS, DQS ,STQC/ DeitY etc.

Number of Certificates Per Country

Japan	4152	Netherlands	24	Belgium	3
UK	573	Saudi Arabia	24	Gibraltar	3
India	546	UAE	19	Lithuania	3
Taiwan	461	Bulgaria	18	Macau	3
China	393	Iran	18	Albania	3
Germany	228	Portugal	18	Bosnia Herzegovina	2
Czech Republic	112	Argentina	17	Cyprus	2
Korea	107	Philippines	16	Ecuador	2
USA	105	Indonesia	15	Jersey	2
Italy	82	Pakistan	15	Kazakhstan	2
Spain	72	Colombia	14	Luxembourg	2
Hungary	71	Russian Federation	14	Macedonia	2
Malaysia	66	Vietnam	14	Malta	2
Poland	61	Iceland	13	Mauritius	2
Thailand	59	Kuwait	11	Ukraine	2
Greece	50	Canada	10	Armenia	1
Ireland	48	Norway	10	Bangladesh	1
Austria	42	Sweden	10	Belarus	1
Turkey	35	Switzerland	9	Bolivia	1
Turkey	35	Bahrain	8	Denmark	1
France	34	Peru	7	Estonia	1
Hong Kong	32	Chile	5	Kyrgyzstan	1
Australia	30	Egypt	5	Lebanon	1
Singapore	29	Oman	5	Moldova	1
Croatia	27	Qatar	5	New Zealand	1
Slovenia	26	Sri Lanka	5	Sudan	1
Mexico	25	South Africa	5	Uruguay	1
Slovakia	25	Dominican Republic	4	Yemen	1
Brazil	24	Morocco	4	Total	7940

Global Standards in Information Security Management

08/11/2012

Scope of this presentation

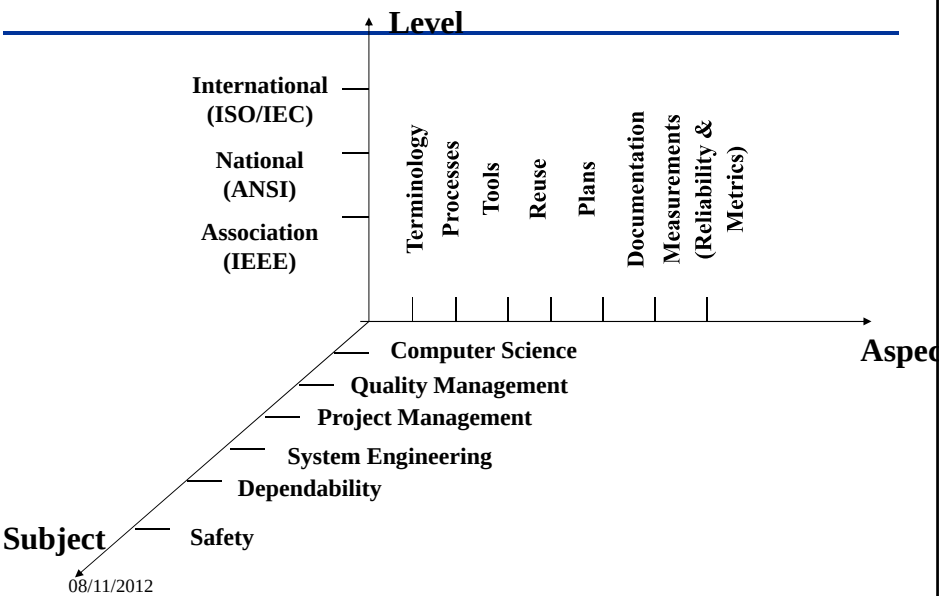
- **Primarily limited to ISO standards (developed as well as being planned) in Information Security and other associated domains and**
- **The role STQC(DIT) is playing w.r.t promotion of these global and National standards in these area.**

08/11/2012

What is a Standard

- **A standard is a document that provides requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose.**

08/11/2012



08/11/2012

Why Standards?

- Bring in industry best practices
- Harmonized approach from definition to implementation to compliance verification
- Common measurement framework
- Reduced cost
- Global acceptance
- …

08/11/2012

Prominent International and National Standards Bodies

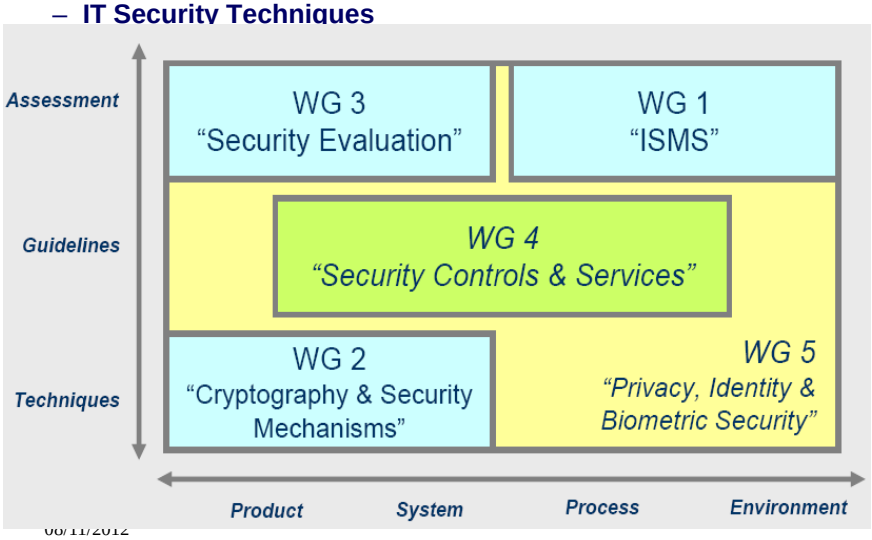
- ISO/IEC (www.iso.ch)
- BSI, UK (www.bsi-global.com)
- NIST, USA (www.nist.gov)
- BIS, India (www.bis.org.in)

DeitY is also developing national standards for e-Governance (www.deity.gov.in)

08/11/20

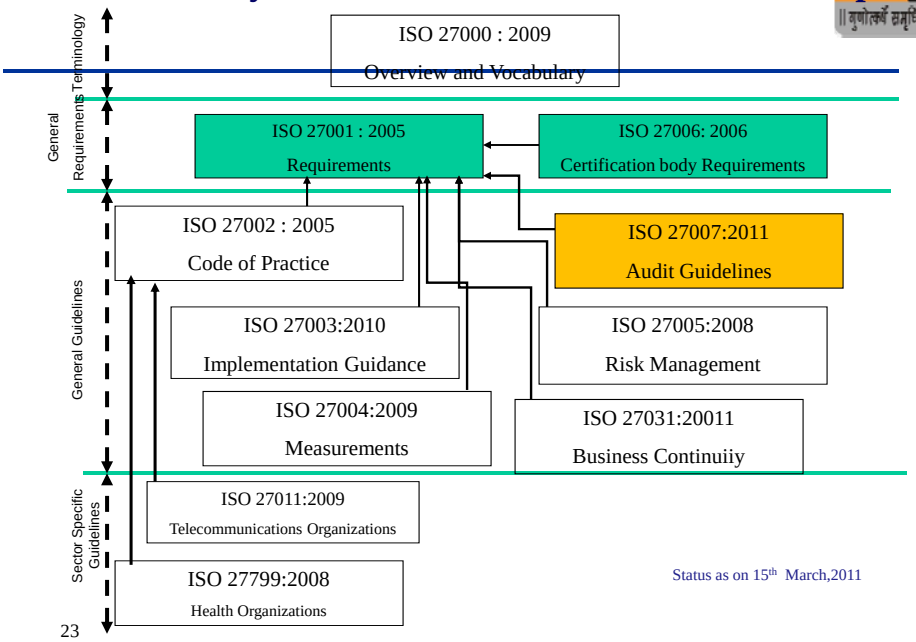
ISO Standards

- **Developed through Sub-Commission JTC1/ SC27**
  - **IT Security Techniques**



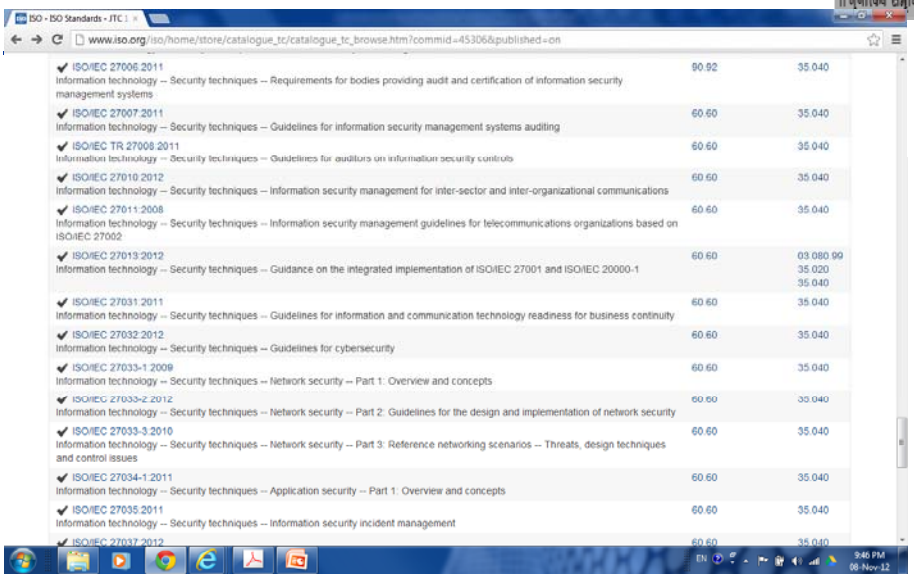
08/11/2012

ISMS family of Standards from ISO : Relationship



23

Other ISMS Published Standards



08/11/2012

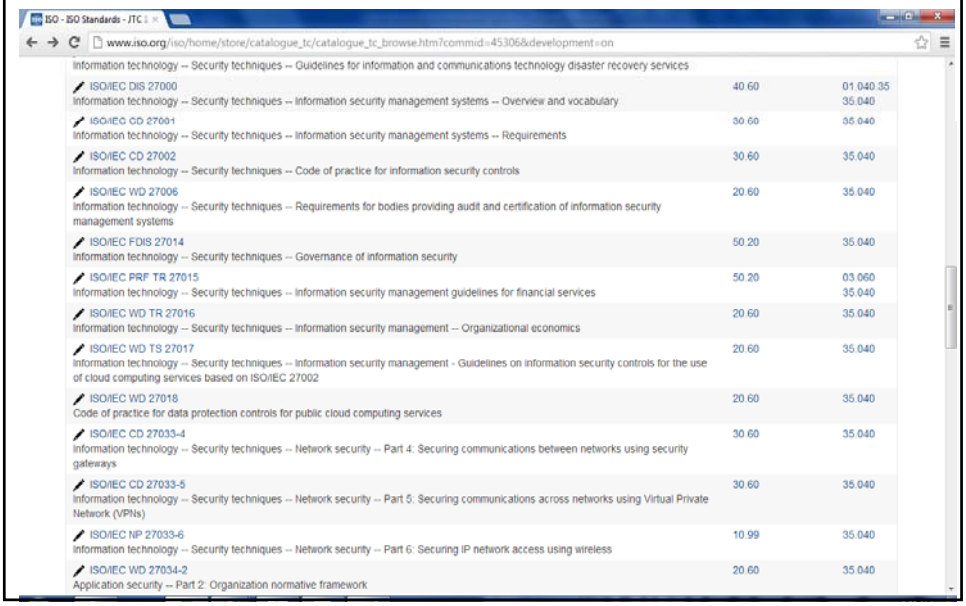
Status as on 8th Nov.,2012

Other Related Standards

- **ISO/IEC 17021**
  - Conformity assessment — Requirements for bodies providing audit and certification of management systems
- **ISO/IEC 19011:2011**
  - **Guidelines for management system auditing**

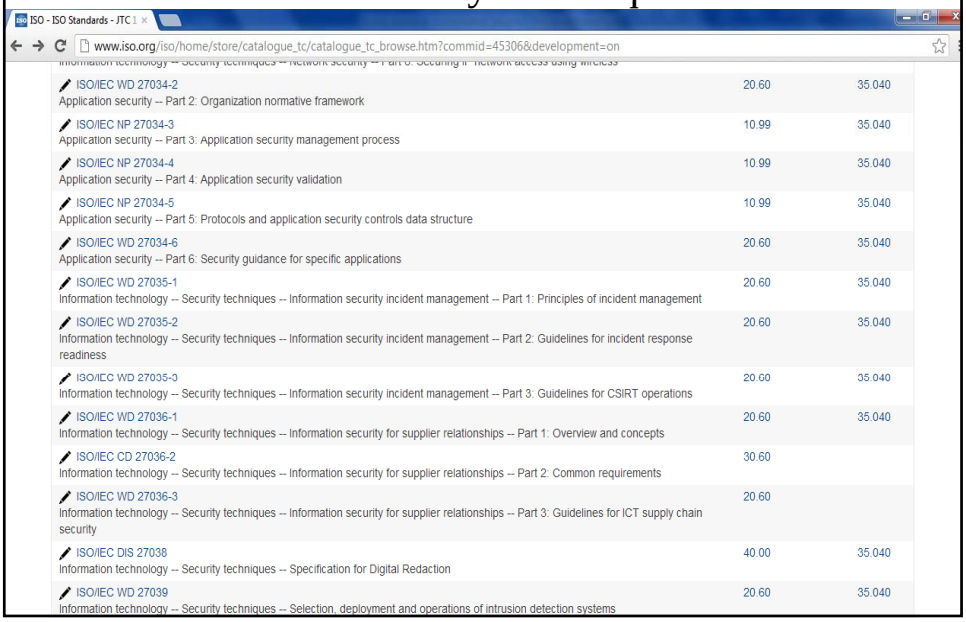
25

Standards being published by ISO JTC1/ SC27 IT Security Techniques



Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services		
ISO/IEC DIS 27000 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary	40.60	01.040.35 35.040
ISO/IEC CD 27001 Information technology -- Security techniques -- Information security management systems -- Requirements	30.60	35.040
ISO/IEC CD 27002 Information technology -- Security techniques -- Code of practice for information security controls	30.60	35.040
ISO/IEC WD 27006 Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems	20.60	35.040
ISO/IEC FDIS 27014 Information technology -- Security techniques -- Governance of information security	50.20	35.040
ISO/IEC PRF TR 27015 Information technology -- Security techniques -- Information security management guidelines for financial services	50.20	03.060 35.040
ISO/IEC WD TR 27016 Information technology -- Security techniques -- Information security management -- Organizational economics	20.60	35.040
ISO/IEC WD TS 27017 Information technology -- Security techniques -- Information security management - Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002	20.60	35.040
ISO/IEC WD 27018 Code of practice for data protection controls for public cloud computing services	20.60	35.040
ISO/IEC CD 27033-4 Information technology -- Security techniques -- Network security -- Part 4: Securing communications between networks using security gateways	30.60	35.040
ISO/IEC CD 27033-5 Information technology -- Security techniques -- Network security -- Part 5: Securing communications across networks using Virtual Private Network (VPNs)	30.60	35.040
ISO/IEC NP 27033-6 Information technology -- Security techniques -- Network security -- Part 6: Securing IP network access using wireless	10.99	35.040
ISO/IEC WD 27034-2 Application security -- Part 2: Organization normative framework	20.60	35.040

Standards being published by ISO JTC1/ SC27 IT Security Techniques



ISO/IEC WD 27034-2 Application security -- Part 2: Organization normative framework	20.60	35.040
ISO/IEC NP 27034-3 Application security -- Part 3: Application security management process	10.99	35.040
ISO/IEC NP 27034-4 Application security -- Part 4: Application security validation	10.99	35.040
ISO/IEC NP 27034-5 Application security -- Part 5: Protocols and application security controls data structure	10.99	35.040
ISO/IEC WD 27034-6 Application security -- Part 6: Security guidance for specific applications	20.60	35.040
ISO/IEC WD 27035-1 Information technology -- Security techniques -- Information security incident management -- Part 1: Principles of incident management	20.60	35.040
ISO/IEC WD 27035-2 Information technology -- Security techniques -- Information security incident management -- Part 2: Guidelines for incident response readiness	20.60	35.040
ISO/IEC WD 27035-3 Information technology -- Security techniques -- Information security incident management -- Part 3: Guidelines for CSIRT operations	20.60	35.040
ISO/IEC WD 27036-1 Information technology -- Security techniques -- Information security for supplier relationships -- Part 1: Overview and concepts	20.60	35.040
ISO/IEC CD 27036-2 Information technology -- Security techniques -- Information security for supplier relationships -- Part 2: Common requirements	30.60	
ISO/IEC WD 27036-3 Information technology -- Security techniques -- Information security for supplier relationships -- Part 3: Guidelines for ICT supply chain security	20.60	
ISO/IEC DIS 27038 Information technology -- Security techniques -- Specification for Digital Redaction	40.00	35.040
ISO/IEC WD 27039 Information technology -- Security techniques -- Selection, deployment and operations of intrusion detection systems	20.60	35.040

BSI Guidelines Documents on ISMS

- **BIP 0071**
  - **Guidelines on requirements and preparation for ISMS certification based on ISO/IEC 27001**
- **BIP 0072**
  - **Are you ready for ISMS audit based on ISO/IEC 27001:2005?**
- **BIP 0073**
  - **Guide to the implementation and auditing of ISMS controls based on ISO/IEC 27001**
- **BIP 0074**
  - **Measuring the effectiveness of your ISMS implementations based on ISO/IEC 27001**

08/11/2012

Security related management systems

- **Software engineering Standards**
  - **Quality management and software life cycle**
    - **ISO 90003**
- **IT Service management**
  - **IT Service management Standards**
    - **ISO/IEC 20000-1(Certification)**
    - **ISO/IEC 20000-2 (Code of practice)**
  - **Supporting Standard**
    - **ITIL – IT Infrastructure Library (version 3)**

08/11/2012

Information Security Standards being published by DIT

- E-Governance_Information_Security_Standard
- Base line security requirements & Selection of controls

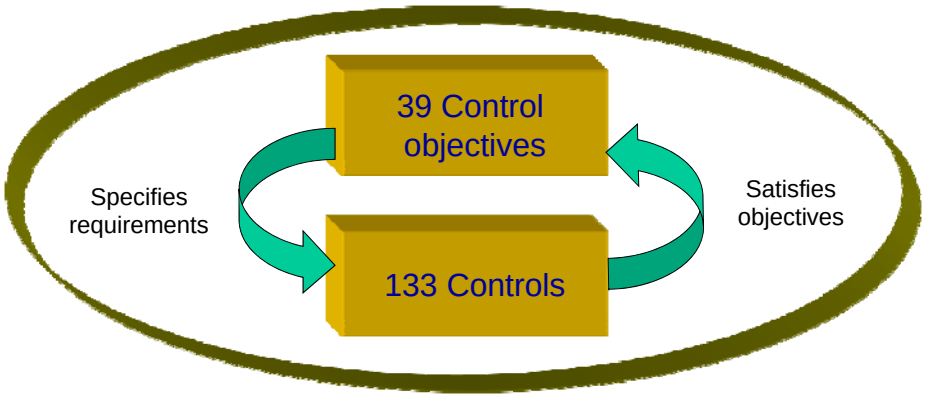
08/11/2012

Conclusion

- ~~ISO 27001 is an umbrella standard and well require~~ many other standards for its effective implementation.
- There is a trend in Security standards from more generic to sector specific.
- The work is going on on integration of ISO 27001 and ISO 20000-1 on IT Service Management
- ISO is developing standards covering almost all aspects of Information security including guideline standards, requirements standards and technology standards.
- It is always easier to adopt (copying) and adapt and then start form beginning
- ISO standards are good source for "*copying*"
  - Basic vision, what and how can be used, is needed

08/11/2012

ISO 27001: Control objectives and controls



11 Security Control clauses

November 9, 2012 Overview of Information Security

ISO 27001 Security Control Domains

- A.5 Security Policy
- A.6 Organization of Information Security
- A.7 Asset Management
- A.8 Human Resources Security
- A.9 Physical & environmental security
- A.10 Communications & operations management
- A.12 Info. Systems Acquisition development & maintenance
- A.11 Access control
- A.13 Information Security Incident Management
- A.14 Business Continuity Management
- A.15 Compliance

08/11/2012

ISMS Implementation

ISMS Standards

- **ISO/ IEC 27001 : 2005**
  - **A specification (specifies requirements for implementing, operating, monitoring, reviewing, maintaining & improving a documented ISMS)**
  - **Specifies the requirements of implementing of Security control, customised to the needs of individual organisation or part thereof.**
  - **Used as a basis for certification**
- **ISO/IEC 27002 : 2005 (Originally 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**

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

Typical 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 a
- 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

Typical 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 Organization
  - Training
  - BCP Testing and Updation

Typical Action Plan for ISMS Implementation-3

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

Issues observed during ISMS audits and experience

Note: *These issues are representative only. They are not the only issues as well as they may not be applicable to many organisations*

ISMS Improvements

Improvements resulting because of ISMS Compliance/ Audits

- Business has become a become a big driver to force an ISMS. Periodic audits by customers.
- Management Commitment for Information security. (Investment in technology, processes and people).
- Awareness at all levels. Awareness of key policies.
- Policies and procedures being understood, documented and implemented.
- BCP. Investment in creating redundancies and BCP/ DR sites; Drills;
- Building Management System
- Vulnerability assessment and the penetration testing
- Strong Security architecture; Centralized patch and Anti-Virus management System

Improvements resulting because of ISMS Compliance/ Audits

- Physical frisking in some industry on sampling basis and acceptance of the same (Cultural change)
- Improved password management system
- Putting SLAs and security Requirements in third party contracts. Earlier emphasis was only on financial aspects.
- Third party Outsourcing : The emphasis has already shifted from just financial to Technical and Financial terms and conditions. SLAs are now being specified. Monitoring has also started.
- Audits of third party and improvement in their security.

Information Security management System has become part of Organisational culture

Issues where improvement SCOPE IS POSSBLE

Process Framework level

- **Defining ISMS Scope and Objectives**
  - **Particularly in the context of Non-IT companies (IT deptt. Or whole organisation)**
  - **When the organisation under Scope is part of a bigger group and when the corporate/ Hqrs/ Parent company is not under scope or when your IT operations/ ISP happens to your own group company (internal outsourcing)**
- **Document control by QA Vs IT departments**
- **Integration of Doc. Control, Internal Audit & CA/PA procedures with other management systems.**
- **Internal audit coverage particularly for CISO functions and outsourcing functions (SLA)**
- **Measurement and Metrics program**
- **Corrective actions/ Preventive actions**
  - **Weak CA/PA. Mostly "corrections" in audit follow-up and not CA.**

Process Framework level

Risk Assessment

- **A well documented, comprehensive and "Useful" risk Assessment is still a concern.**
- **Actual risk assessment findings and its co-relation with selection and extent of controls to be applied**
- **Repeatability and reproducibility of results**
- **Methodology, resolution for various levels of risk & residual risk**
- **Completeness in terms of assets identification (particularly those located offsite)**
- **Comprehensiveness of threats & vulnerabilities**

Internal Audits

- **NCs are raised against Standard and not against Organisation's own documents, policies. Such NCs are unfriendly to the users and they avoid their closure.**
- **Sometimes NCs are not understood by them; agreed by them and hence not closed.**
-

Asset management

- **Completeness of Asset Register. (Services,Applications developed, databases & offsite facilities sometimes missing).**
- **Asset classification levels (either too simple to give any value or too complex to implement)**
- **Information labeling and Handling not as per the Asset Classification,…. Procedure (e records- life cycle)**
- **Sometimes same asset classification changes with time. This provision is mostly missing.**

Security Organizational and other HR Issues

- **When IT driven, Process framework clauses; HR and Admin. Policies procedures take a back seat.**
- **When QA driven, the last level integration of IT procedures/ Technology documents with the ISMS gets missed(FMS- procedures)**
- **After certification, the initial euphoria is over; The project moves in its "Maintenance" phase and it is handed over to the junior team, who are not able to push the issues forcefully. The "Periodic Audit/ Review" become more of a formality.**
- **Reviews of NDAs , SLAs and Terms and Conditions and its awareness to employees.**
- **Withdrawal of IDs and access rights and its periodic review.**
- **The Screening and background checks done sometimes through "Unorganized" sector.**

Physical and Env. Security

- Tailgating
- Control of access cards and records including when the person is released and redeployed
- Access of third party personnel
- Clock Synchronization in BMS systems
- Resolution of CCTVs in the event of thefts
- Training/ knowledge of physical security procedures to security personnel (generally outsourced function)
- Testing and trainings of DR plans

Technical Controls

- Integration of Technical documents with the ISMS
- User Access Review
- Testing of back-up data
- Password policy
- Administrator rights to local users with few/no desktop reviews.
- Firewall configurations not maintained properly. Common Network (e.g. Firewall) and System administrators
- Security Testing of applications already in use/ or when developed "internally" by a group belonging to the same organization but not under the scope.

Incident Reporting and Follow-up

- Incident database
- Difference between Incidents and events/ normal faults
- Recording of incidents particularly IT incidents
- Incident Analysis
- Learning from incidents and communication

BCM Issues

- Formal BIA
- Coverage of BCP/ DR activities (multiple locations)
- Co-relation of RTO and RPO with the contractual need of the projects
- BCP Testing
- Review and Upgradation

Project Security Requirements

- No consolidation of Client Security Requirements, which can give inputs to HR, Project level BCP/DR, Physical
- Client Security requirements also keep changing or atleast the perception and hence the organisation need to maintain it also.

Compliance

- List of applicable legislation – The knowledge, its relevance to ISMS scope
- While IT act 2000 is shown to be applicable by most companies. How its compliance is ensured by the company is not known
- "Contractual requirements" are normally not stated
- Technical compliance Audit
- Desktop compliance Audit – Frequency; checklist as well as the sample size
- Security of records stored in Electronic form

The Clauses/ domains where the issues are mostly observed

- Risk management
- Asset management
- HR/Resources (Awareness/ Training)
- Physical Security
- BCP
- Service management
- Management of Outsourcing partners

Issues and Challenges

- Organization Priorities of Certification Vs. Certificate. Certification as a managed function??
- Fast Changing Functional and Security Organization
- You are part of a bigger organization and hence difficult to implement / manage ISMS.
- Integration of Corporate/ Global polices with local ones.
- Shared Services across organization well beyond the scope of certification.

Conclusion

- **ISMS compliance and ISO 27001 certification is picking up in India very fast. Business reasons are there.**
- **Effective ISMS implementation requires strong Management Commitment and Support.**
- **ISMS is now seen as a necessity and a lot of Security improvements have happened in the organizations.**
- **ISO 27001 can not be effectively implemented in isolation. Other Guideline, Technology and assessment standards covering Products, Processes, Systems and Environment standards as appropriate have to be seen and applied within the context of overall scope.**
- **The new developments are putting increasing emphasis on measurement and improvement of ISMS. Area specific standards are being developed.**

Thank U for your attention!

Arvind Kumar arvind@mit.gov.in