Gap Analysis: Status of ISO 27001 Implementation

ISO 27001 clause	Mandatory requirement for the ISMS
4	**Information Security Management System**
4.1	**General requirements**
4.1	The organization shall establish, implement, operate, monitor, review, maintain and improve a documented ISMS
4.2	**Establishing and managing the ISMS**
4.2.1	**Establish the ISMS**
4.2.1 (a)	Define the scope and boundaries of the ISMS
4.2.1 (b)	Define an ISMS policy
4.2.1 (c)	Define the risk assessment approach
4.2.1 (d)	Identify the risks
4.2.1 (e)	Analyse and evaluate the risks
4.2.1 (f)	Identify and evaluate options for the treatment of risks
4.2.1 (g)	Select control objectives and controls for the treatment of risks
4.2.1 (h)	Obtain management approval of the proposed residual risks
4.2.1 (i)	Obtain management authorization to implement and operate the ISMS
4.2.1 (j)	Prepare a Statement of Applicability [see the SoA spreadsheet]
4.2.2	**Implement the ISMS**
4.2.2 (a)	Formulate a risk treatment plan
4.2.2 (b)	Implement the risk treatment plan in order to achieve the identified control objectives
4.2.2 (c)	Implement controls selected in 4.2.1g to meet the control objectives
4.2.2 (d)	Define how to measure the effectiveness of the selected controls or groups of controls and specify how these measurements are to be used to assess control effectiveness to produce comparable and reproducible results (see 4.2.3c)
4.2.2 (e)	Implement training and awareness programmes (see 5.2.2)
4.2.2 (f)	Manage operation of the ISMS
4.2.2 (g)	Manage resources for the ISMS (see 5.2)
4.2.2 (h)	Implement procedures and other controls capable of enabling prompt detection of security events and response to security incidents (see 4.2.3a)
4.2.3	**Monitor and review the ISMS**
4.2.3 (a)	Execute monitoring and reviewing procedures and other controls
4.2.3 (b)	Undertake regular reviews of the effectiveness of the ISMS
4.2.3 (c)	Measure the effectiveness of controls to verify that security requirements have been met.
4.2.3 (d)	Review risk assessments at planned intervals and review the residual risks and the identified acceptable levels of risks
4.2.3 (e)	Conduct internal ISMS audits at planned intervals (see 6)
4.2.3 (f)	Undertake a management review of the ISMS on a regular basis (see 7.1)
4.2.3 (g)	Update security plans to take into account the findings of monitoring and reviewing activities
4.2.3 (h)	Record actions and events that could have an impact on the effectiveness or performance of the ISMS (see 4.3.3)
4.2.4	**Maintain and improve the ISMS**
4.2.4 (a)	Implement the identified improvements in the ISMS.
4.2.4 (b)	Take appropriate corrective and preventive actions in accordance with 8.2 and 8.3
4.2.4 (c)	Communicate the actions and improvements to all interested parties
4.2.4 (d)	Ensure that the improvements achieve their intended objectives
4.3	**Documentation requirements**
4.3.1	**General ISMS documentation**

4.3.1 (a)	Documented statements of the ISMS policy (see 4.2.1b) and objectives
4.3.1 (b)	Scope of the ISMS (see 4.2.1a)
4.3.1 (c)	Procedures and controls in support of the ISMS
4.3.1 (d)	Description of the risk assessment methodology (see 4.2.1c)
4.3.1 (e)	Risk assessment report (see 4.2.1c to 4.2.1g)
4.3.1 (f)	Risk treatment plan (see 4.2.2b)
4.3.1 (g)	Procedures needed by the organization to ensure the effective planning, operation and control of its information security processes and describe how to measure the effectiveness of controls (see 4.2.3c)
4.3.1 (h)	Records required by this International Standard (see 4.3.3)
4.3.1 (i)	Statement of Applicability
4.3.2	**Control of documents**
4.3.2	Documents required by the ISMS shall be protected and controlled. A documented procedure shall be established to define the management actions needed to:
4.3.2 (a)	Approve documents for adequacy prior to issue
4.3.2 (b)	Review and update documents as necessary and re-approve documents
4.3.2 (c)	Ensure that changes and the current revision status of documents are identified
4.3.2 (d)	Ensure that relevant versions of applicable documents are available at points of use
4.3.2 (e)	Ensure that documents remain legible and readily identifiable
4.3.2 (f)	Ensure that documents are available to those who need them, and are transferred, stored and ultimately disposed of in accordance with the procedures applicable to their classification
4.3.2 (g)	Ensure that documents of external origin are identified
4.3.2 (h)	Ensure that the distribution of documents is controlled
4.3.2 (i)	Prevent the unintended use of obsolete documents
4.3.2 (j)	Apply suitable identification to documents if they are retained for any purpose
4.3.3	**Control of records**
4.3.3	Records shall be established and maintained to provide evidence of conformity to requirements and the effective operation of the ISMS …
4.3.3	Records shall be protected and controlled.
4.3.3	The ISMS shall take account of any relevant legal or regulatory requirements and contractual obligations.
4.3.3	Records shall remain legible, readily identifiable and retrievable.
4.3.3	The controls needed for the identification, storage, protection, retrieval, retention time and disposition of records shall be documented and implemented.
4.3.3	Records shall be kept of the performance of the process as outlined in 4.2 and of all occurrences of significant security incidents related to the ISMS.
5	**Management responsibility**
5.1	**Management commitment**
5.1	Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:
5.1 (a)	Establishing an ISMS policy
5.1 (b)	Ensuring that ISMS objectives and plans are established
5.1 (c)	Establishing roles and responsibilities for information security
5.1 (d)	Communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement
5.1 (e)	Providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS (see 5.2.1)
5.1 (f)	Deciding the criteria for accepting risks and the acceptable levels of risk

5.1 (g)	Ensuring that internal ISMS audits are conducted (see 6)
5.1 (h)	Conducting management reviews of the ISMS (see 7)
5.2	**Resource management**
5.2.1	**Provision of resources**
5.2.1	The organization shall determine and provide the resources needed to:
5.2.1 (a)	Establish, implement, operate, monitor, review, maintain and improve an ISMS
5.2.1 (b)	Ensure that information security procedures support the business requirements
5.2.1 (c)	Identify and address legal and regulatory requirements and contractual security obligations
5.2.1 (d)	Maintain adequate security by correct application of all implemented controls
5.2.1 (e)	Carry out reviews when necessary, and to react appropriately to the results of these reviews
5.2.1 (f)	Where required, improve the effectiveness of the ISMS
5.2.2	**Training, awareness and competence**
5.2.2	The organization shall ensure that all personnel who are assigned responsibilities defined in the ISMS are competent to perform the required tasks by:
5.2.2 (a)	Determining the necessary competencies for personnel performing work effecting the ISMS
5.2.2 (b)	Providing training or taking other actions (e.g. employing competent personnel) to satisfy these needs
5.2.2 (c)	Evaluating the effectiveness of the actions taken
5.2.2 (d)	Maintaining records of education, training, skills, experience and qualifications (see 4.3.3)
5.2.2	The organization shall also ensure that all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives.
6	**Internal ISMS audit**
6	The organization shall conduct internal ISMS audits at planned intervals to determine whether the control objectives, controls, processes and procedures of its ISMS:
6 (a)	Conform to the requirements of this International Standard and relevant legislation or regulations
6 (b)	Conform to the identified information security requirements
6 (c)	Are effectively implemented and maintained
6 (d)	Perform as expected.
6	An audit programme shall be planned
6	The management responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected nonconformities and their causes. Follow-up activities shall include the verification of the actions taken and the reporting of verification results (see 8).
7	**Management review of the ISMS**
7.1	**General**
7.1	Management shall review the organization's ISMS at planned intervals (at least once a year) to ensure its continuing suitability, adequacy and effectiveness
7.2	**Review input**
7.2	The input to a management review shall include:
7.2 (a)	Rsults of ISMS audits and reviews
7.2 (b)	Feedback from interested parties
7.2 (c)	Techniques, products or procedures, which could be used in the organization to improve the ISMS performance and effectiveness

7.2 (d)	Status of preventive and corrective actions
7.2 (e)	Vulnerabilities or threats not adequately addressed in the previous risk assessment
7.2 (f)	Results from effectiveness measurements
7.2 (g)	Follow-up actions from previous management reviews
7.2 (h)	Any changes that could affect the ISMS
7.2 (i)	Recommendations for improvement
7.3	**Review output**
7.3	The output from the management review shall include any decisions and actions related to the following:
7.3 (a)	Improvement of the effectiveness of the ISMS
7.3 (b)	Update of the risk assessment and risk treatment plan
7.3 (c)	Modification of procedures and controls that effect information security, as necessary, to respond to internal or external events that may impact on the ISMS
7.3 (d)	Resource needs
7.3 (e)	Improvement to how the effectiveness of controls is being measured
8	**ISMS improvement**
8.1	**Continual improvement**
8.1	The organization shall continually improve the effectiveness of the ISMS through the use of the information security policy, information security objectives, audit results, analysis of monitored events, corrective and preventive actions and management review (see 7).
8.2	**Corrective action**
8.2	The organization shall take action to eliminate the cause of nonconformities with the ISMS requirements in order to prevent recurrence. The documented procedure for corrective action shall define requirements for:
8.2 (a)	Identifying nonconformities
8.2 (b)	Determining the causes of nonconformities
8.2 (c)	Evaluating the need for actions to ensure that nonconformities do not recur
8.2 (d)	Determining and implementing the corrective action needed
8.2 (e)	Recording results of action taken (see 4.3.3)
8.2 (f)	Reviewing of corrective action taken
8.3	**Preventive action**
8.3	The organization shall determine action to eliminate the cause of potential nonconformities with the ISMS requirements in order to prevent their occurrence. Preventive actions taken shall be appropriate to the impact of the potential problems. The documented procedure for preventive action shall define requirements for:
8.3 (a)	Identifying potential nonconformities and their causes
8.3 (b)	Evaluating the need for action to prevent occurrence of nonconformities
8.3 (c)	Determining and implementing preventive action needed
8.3 (d)	Recording results of action taken (see 4.3.3)
8.3 (e)	Reviewing of preventive action taken
8.3	The organization shall identify changed risks and identify preventive action requirements focusing attention on significantly changed risks

Status	Look for
D	
D	
D	
D	
RD	
RD	
RD	
D	
RD	
RD	
D	
RD	
RD	
RD	
RD	
RD	
RD	
RD	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	

RD	
D	
D	
D	
D	
D	
D	
D	
D	
RD	
RD	
RD	
RD	
RD	
RD	
RD	
RD	
RD	
RD	
RD	
RD	
RD	
RD	
RD	
RD	
RD	
PNP	
RD	
PNP	
PNP	
PNP	
PNP	
PNP	

PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
RD	
PNP	
PNP	
PNP	
D	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	

PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
PNP	
D	
NA	
PNP	
PNP	
PNP	
RD	
PNP	
RD	
PNP	
PNP	
PNP	
MD	

Findings

Remarks / Recommendations

Statement of Applicability of ISO/IEC 27001 Annex A controls					
Annex A reference	**Control title**	**Control description**	**Function**	**Status**	**Look for**
A.5	**Security Policy**				
A5.1	**Information security policy**	**To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.**			
A.5.1.1	Information security policy document	An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties.	Top Management	**RD**	
A.5.1.2	Review of the information security policy	The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.	Top Management	**D**	
A.6	**Organization of information security**				
A.6.1	**Internal Organization**	**To manage information security within the organization.**			
A.6.1.1	Management commitment to information security	Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security responsibilities.	Top Management	**PNP**	
A.6.1.2	Information security coordination	Information security activities shall be co-ordinated by representatives from different parts of the organization with relevant roles and job function.	CISO	**RD**	
A.6.1.3	Allocation of information security responsibilities	All information security responsibilities shall be clearly defined.	HR	**MD**	
A.6.1.4	Authorization process for information processing facilities	A management authorization process for new information processing facilities shall be defined and implemented.	CISO	**NA**	
A.6.1.5	Confidentiality agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified and regularly reviewed.	CISO	**D**	
A.6.1.6	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	Administration	**D**	
A.6.1.7	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	IT	**D**	
A.6.1.8	Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes to the security implementation occur.	CISO	**D**	
A6.2	**External parties**	**To maintain the security of organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.**			
A.6.2.1	Identification of risks related to external parties	The risks to the organization's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.	CISO	**D**	
A.6.2.2	Addressing security when dealing with customers	All identified security requirements shall be addressed before giving customers access to the organization's information or assets.	IT	**D**	
A.6.2.3	Addressing security in third party contracts	Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.	Finance	**D**	
A.7	**Asset Management**				
A.7.1	**Responsibility for assets**	**To achieve and maintain appropriate protection of organizational assets.**			
A.7.1.1	Inventory of assets	All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.	CISO	**D**	
A.7.1.2	Ownership of assets	All information and assets associated with information processing facilities shall be owned by a designated part of the organization.	CISO	**D**	

Annex A reference	Control title	Control description	Function	Status	Look for
A.7.1.3	Acceptable use of assets	Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.	CISO	**D**	
A.7.2	**Information classification**	**To ensure that information receives an appropriate level of protection.**			
A.7.2.1	Classification guidelines	Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization.	CISO	**D**	
A.7.2.2	Information labelling and handling	An appropriate set of procedures for information labelling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization.	CISO	**D**	
A.8	**Human resources security**				
A.8.1	**Prior to employment**	**To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.**			
A.8.1.1	Roles and responsibilities	Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy.	HR	**D**	
A.8.1.2	Screening	Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.	HR	**D**	
A.8.1.3	Terms and conditions of employment	As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for information security.	HR	**D**	
A.8.2	**During employment**	**To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.**			
A.8.2.1	Management responsibilities	Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.	HR	**D**	
A.8.2.2	Information security awareness, education and training	All employees of the organization and, where relevant, contractors and third-party users, shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.	Training	**D**	
A.8.2.3	Disciplinary process	There shall be a formal disciplinary process for employees who have committed a security breach.	HR	**D**	
A.8.3	**Termination or change of employment**	**To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.**			
A.8.3.1	Termination responsibilities	Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.	HR	**D**	
A.8.3.2	Return of assets	All employees, contractors and third party users shall return all of the organization's assets in their possession upon termination of their employment, contract or agreement.	HR	**D**	
A.8.3.3	Removal of access rights	The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	HR	**D**	
A.9	**Physical and environmental security**				
A9.1	**Secure areas**	**To prevent unauthorized physical access, damage and interference to the organization's premises and information.**			

Annex A reference	Control title	Control description	Function	Status	Look for
A9.1.1	Physical security perimeter	Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities.	Administration	**D**	
A9.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Administration	**D**	
A9.1.3	Securing offices, rooms and facilities	Physical security for offices, rooms, and facilities shall be designed and applied	Administration	**D**	
A9.1.4	Protecting against external and environmental threats	Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied.	Administration	**D**	
A9.1.5	Working in secure areas	Physical protection and guidelines for working in secure areas shall be designed and applied.	Administration	**D**	
A9.1.6	Public access, delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	Administration	**D**	
A9.2	**Equipment security**	**To prevent loss, damage, theft or compromise of assets and interruption to organization's activities.**			
A9.2.1	Equipment siting and protection	Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	Administration	**D**	
A9.2.2	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Administration	**D**	
A9.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.	Administration	**D**	
A9.2.4	Equipment maintenance	Equipment shall be correctly maintained to enable its continued availability and integrity.	IT	**D**	
A9.2.5	Security of equipment off-premises	Security shall be applied to off-site equipment taking into account the different risks of working outside the organization's premises.	IT	**D**	
A9.2.6	Secure disposal or re-use of equipment	All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.	IT	**D**	
A9.2.7	Removal of property	Equipment, information or software shall not be taken off-site without prior authorization.	Administration	**D**	
A10	**Communications and operations management**				
A10.1	**Operational procedures and responsibilities**	**To ensure the correct and secure operation of information processing facilities.**			
A10.1.1	Documented operating procedures	Operating procedures shall be documented, maintained, and made available to all users who need them.	CISO	**D**	
A10.1.2	Change management	Changes to information processing facilities and systems shall be controlled.	CISO	**D**	
A10.1.3	Segregation of duties	Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	CISO	**D**	
A10.1.4	Separation of development, test and operational facilities	Development, test and operational facilities shall be separated to reduce the risks of unauthorized access or changes to the operational system.	CISO	**D**	
A10.2	**Third party service delivery management**	**To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.**			
A10.2.1	Service Delivery	It shall be ensured that the security controls, service definitions, and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.	CISO	**D**	
A10.2.2	Monitoring and review of third party services	The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.	CISO	**D**	

Annex A reference	Control title	Control description	Function	Status	Look for
A10.2.3	Managing changes to third party services	Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.	CISO	**D**	
A10.3	**System planning and acceptance**	**To minimize the risk of systems failure.**			
A10.3.1	Capacity management	The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.	IT	**D**	
A10.3.2	System acceptance	Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system's) carried out during development and prior to acceptance.	IT	**D**	
A10.4	**Protection against malicious and mobile code**	**To protect the integrity of software and information.**			
A10.4.1	Controls against malicious code	Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.	IT	**D**	
A10.4.2	Controls against mobile code	Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code shall be prevented from executing.	IT	**D**	
A10.5	**Back-up**	**To maintain the integrity and availability of information and information processing facilities.**			
A10.5.1	Information back-up	Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.	IT	**D**	
A10.6	**Network security management**	**To ensure the protection of information in networks and the protection of the supporting infrastructure.**			
A10.6.1	Network controls	Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.	IT	**D**	
A10.6.2	Security of network services	Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.	IT	**D**	
A10.7	**Media handling**	**To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.**			
A10.7.1	Management of removable media	There shall be procedures in place for the management of removable media.	Administration	**D**	
A10.7.2	Disposal of media	Media shall be disposed of securely and safely when no longer required, using formal procedures.	Administration	**D**	
A10.7.3	Information handling procedures	Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse.	Administration	**D**	
A10.7.4	Security of system documentation	System documentation shall be protected against unauthorized access.	IT	**D**	
A10.8	**Exchange of information**	**To maintain the security of information and software exchanged within an organization and with any external entity.**			
A10.8.1	Information exchange policies and procedures	Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities.	CISO	**D**	
A10.8.2	Exchange agreements	Agreements shall be established for the exchange of information and software between the organization and external parties.	CISO	**D**	
A10.8.3	Physical media in transit	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.	Administration	**D**	
A10.8.4	Electronic messaging	Information involved in electronic messaging shall be appropriately protected.	CISO	**D**	
A10.8.5	Business information systems	Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.	CISO	**D**	

Annex A reference	Control title	Control description	Function	Status	Look for
A10.9	**Electronic commerce services**	**To ensure the security of electronic commerce services, and their secure use.**			
A10.9.1	Electronic commerce	Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.	IT	**D**	
A10.9.2	On-line transactions	Information involved in on-line transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	IT	**D**	
A10.9.3	Publicly available information	The integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification.	IT	**D**	
A10.10	**Monitoring**	**To detect unauthorized information processing activities.**			
A10.10.1	Audit logging	Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.	IT	**D**	
A10.10.2	Monitoring system use	Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.	IT	**D**	
A10.10.3	Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.	IT	**D**	
A10.10.4	Administrator and operator logs	System administrator and system operator activities shall be logged.	IT	**D**	
A10.10.5	Fault logging	Faults shall be logged, analyzed, and appropriate action taken.	IT	**D**	
A10.10.6	Clock synchronization	The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.	IT	**D**	
A11	**Access Control**				
A11.1	**Business requirement for access control**	**To control access to information.**			
A11.1.1	Access control policy	An access control policy shall be established, documented, and reviewed based on business and security requirements for access.	IT	**D**	
A11.2	**User access management**	**To ensure authorized user access and to prevent unauthorized access to information systems.**			
A11.2.1	User registration	There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.	IT	**D**	
A11.2.2	Privilege management	The allocation and use of privileges shall be restricted and controlled.	IT	**D**	
A11.2.3	User password management	The allocation of passwords shall be controlled through a formal management process.	IT	**D**	
A11.2.4	Review of user access rights	Management shall review users' access rights at regular intervals using a formal process.	IT	**D**	
A11.3	**User responsibilities**	**To prevent unauthorized user access, and compromise or theft of information and information processing facilities.**			
A11.3.1	Password use	Users shall be required to follow good security practices in the selection and use of passwords.	IT	**D**	
A11.3.2	Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.	IT	**D**	
A11.3.3	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	IT	**D**	
A11.4	**Network access control**	**To prevent unauthorized access to networked services.**			
A11.4.1	Policy on use of network services	Users shall only be provided with access to the services that they have been specifically authorized to use.	IT	**D**	
A11.4.2	User authentication for external connections	Appropriate authentication methods shall be used to control access by remote users.	IT	**D**	
A11.4.3	Equipment identification in networks	Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.	IT	**D**	
A11.4.4	Remote diagnostic and configuration port protection	Physical and logical access to diagnostic and configuration ports shall be controlled.	IT	**D**	
A11.4.5	Segregation in networks	Groups of information services, users and information systems shall be segregated on networks.	IT	**D**	

Annex A reference	Control title	Control description	Function	Status	Look for
A11.4.6	Network connection control	For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications (see 11.1).	IT	**D**	
A11.4.7	Network routing control	Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.	IT	**D**	
A11.5	**Operating system access control**	**To prevent unauthorized access to operating systems.**			
A11.5.1	Secure log-on procedures	Access to operating systems shall be controlled by a secure log-on procedure.	IT	**D**	
A11.5.2	User identification and authentication	All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.	IT	**D**	
A11.5.3	Password management system	Systems for managing passwords shall be interactive and shall ensure quality passwords.	IT	**D**	
A11.5.4	Use of system utilities	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	IT	**D**	
A11.5.5	Session time-out	Inactive sessions shall be shut down after a defined period of inactivity.	IT	**D**	
A11.5.6	Limitation of connection time	Restrictions on connection times shall be used to provide additional security for high-risk applications.	IT	**D**	
A11.6	**Application and information access control**	**To prevent unauthorized access to information held in application systems.**			
A11.6.1	Information access restriction	Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.	IT	**D**	
A11.6.2	Sensitive system isolation	Sensitive systems shall have a dedicated (isolated) computing environment.	IT	**D**	
A11.7	**Mobile computing and Teleworking**	**To ensure information security when using mobile computing and teleworking facilities.**			
A11.7.1	Mobile computing and communications	A formal policy shall be in place, and security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.	CISO	**D**	
A11.7.2	Teleworking	A policy, operational plans and procedures shall be developed and implemented for teleworking activities.	CISO	**D**	
A12	**Information systems acquisition, development and maintenance**				
A12.1	**Security requirements of information systems**	**To ensure that security is an integral part of information systems.**			
A12.1.1	Security requirements analysis and specification	Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls.	CISO	**D**	
A12.2	**Correct processing in applications**	**To prevent errors, loss, unauthorized modification or misuse of information in application.**			
A12.2.1	Input data validation	Data input to applications shall be validated to ensure that this data is correct and appropriate.	S/W	**D**	
12.2.2	Control of internal processing	Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.	S/W	**D**	
12.2.3	Message integrity	Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.	S/W	**D**	
12.2.4	Output data validation	Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.	S/W	**D**	

Annex A reference	Control title	Control description	Function	Status	Look for
A12.3	**Cryptographic controls**	**To protect the confidentiality, authenticity or integrity of information by cryptographic means.**			
A12.3.1	Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	IT	**D**	
12.3.2	Key management	Key management shall be in place to support the organization's use of cryptographic techniques.	IT	**D**	
A12.4	**Security of system files**	**To ensure the security of system files**			
A12.4.1	Control of operational software	There shall be procedures in place to control the installation of software on operational systems	IT	**D**	
A12.4.2	Protection of system test data	Test data shall be selected carefully, and protected and controlled.	S/W	**D**	
A12.4.3	Access control to program source code	Access to program source code shall be restricted.	S/W	**D**	
A12.5	**Security in development and support processes**	**To maintain the security of application system software and information.**			
A12.5.1	Change control procedures	The implementation of changes shall be controlled by the use of formal change control procedures.	S/W	**D**	
A12.5.2	Technical review of applications after operating system changes	When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	IT	**D**	
A12.5.3	Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.	IT	**D**	
A12.5.4	Information leakage	Opportunities for information leakage shall be prevented.	IT	**D**	
A12.5.5	Outsourced software development	Outsourced software development shall be supervised and monitored by the organization.	S/W	**D**	
A12.6	**Technical Vulnerability Management**	**To reduce risks resulting from exploitation of published technical vulnerabilities.**			
A12.6.1	Control of technical vulnerabilities	Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.	IT	**D**	
A13	**Information security incident management**			**D**	
A13.1	**Reporting information security events and weaknesses**	**To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.**			
A13.1.1	Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.	CISO	**D**	
A13.1.2	Reporting security weaknesses	All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.	CISO	**D**	
A13.2	**Management of information security incidents and improvements**	**To ensure a consistent and effective approach is applied to the management of information security incidents.**			
A13.2.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	CISO	**D**	
A13.2.2	Learning from information security incidents	There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.	CISO	**D**	
A13.2.3	Collection of evidence	Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).	CISO	**D**	
A14	**Business continuity management**				
A14.1	**Information security aspects of business continuity management**	**To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.**			

Annex A reference	Control title	Control description	Function	Status	Look for
A14.1.1	Including information security in the business continuity management process	A managed process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.	CISO	**D**	
A14.1.2	Business continuity and risk analysis	Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.	CISO	**D**	
A14.1.3	Developing and implementing continuity plans including information security	Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.	CISO	**D**	
A14.1.4	Business continuity planning framework	A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.	CISO	**D**	
A14.1.5	Testing, maintaining and re-assessing business continuity plans	Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.	CISO	**D**	
A15	**Compliance**				
A15.1	**Compliance with legal requirements**	**To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.**			
A15.1.1	Identification of applicable legislation	All relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization.	Finance	**D**	
A15.1.2	Intellectual property rights (IPR)	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.	IT	**D**	
A15.1.3	Protection of organizational records	Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.	IT	**D**	
A15.1.4	Data protection and privacy of personal information	Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.	Finance	**D**	
A15.1.5	Prevention of misuse of information processing facilities	Users shall be deterred from using information processing facilities for unauthorized purposes.	Administration	**D**	
A15.1.6	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.	IT	**D**	
A15.2	**Compliance with security policies and standards, and technical compliance**	**To ensure compliance of systems with organizational security policies and standards**			
A15.2.1	Compliance with security policies and standards	Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.	Top Management	**D**	
A15.2.2	Technical compliance checking	Information systems shall be regularly checked for compliance with security implementation standards.	IT	**D**	
A15.3	**Information system audit considerations**	**To maximize the effectiveness of and to minimize interference to/from the information systems audit process.**		**D**	
A15.3.1	Information systems audit controls	Audit requirements and activities involving checks on operational systems shall be planned carefully and agreed to minimize the risk of disruptions to business processes.	IT	**D**	
A15.3.2	Protection of information systems audit tools	Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.	IT	**D**	
Legend					
Count	**Status Code**	**Meaning**		**Contribution %**	

Annex A reference	Control title	Control description	Function	Status	Look for
130	D	Control is documented and implemented		96%	
1	MD	Control is implemented and process must be documented to ensure repeatability of process and mitigate the risks.		1%	
2	RD	Control is not comply with standards and it must be redesigned to comply with standards		1%	
1	PNP	Process is not in place / not implemented. (Required Control is neither documented nor implemented)		1%	
1	NA (Not Applicable)	Control is not applicable for the company as per the business		1%	
135					

Findings	Recommendations

Findings	Recommendations

Findings	Recommendations

Findings	Recommendations

Findings	Recommendations

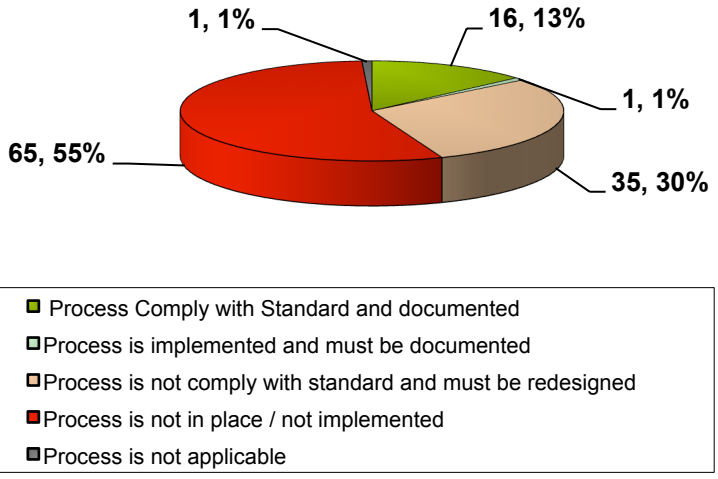
Findings	Recommendations

Findings	Recommendations

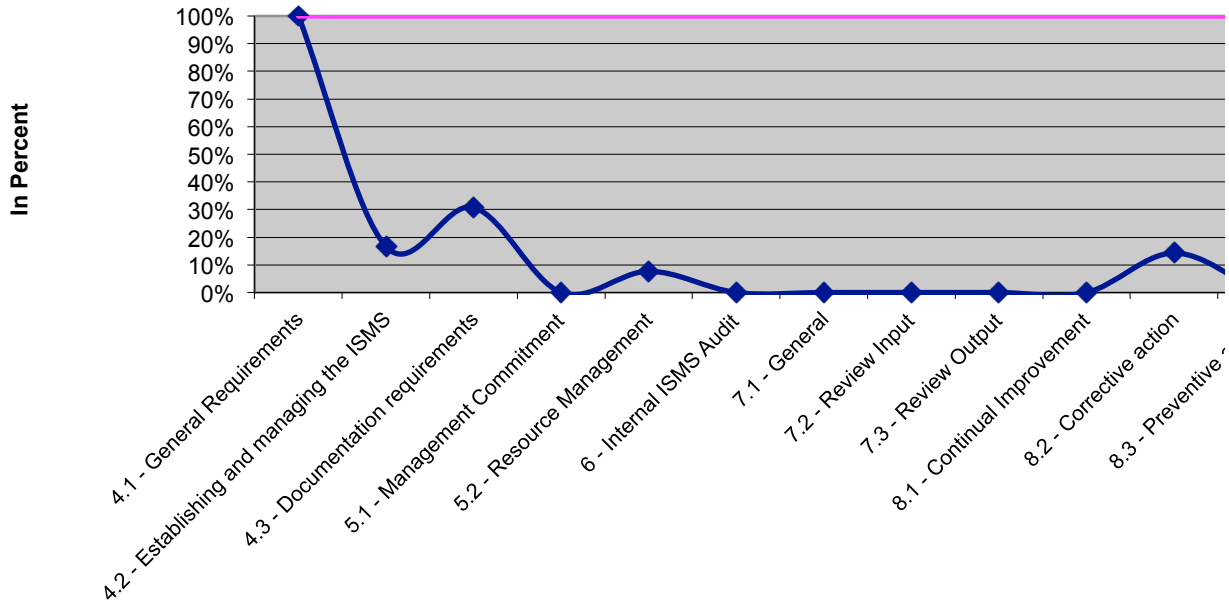
Findings	Recommendations

Findings	Recommendations

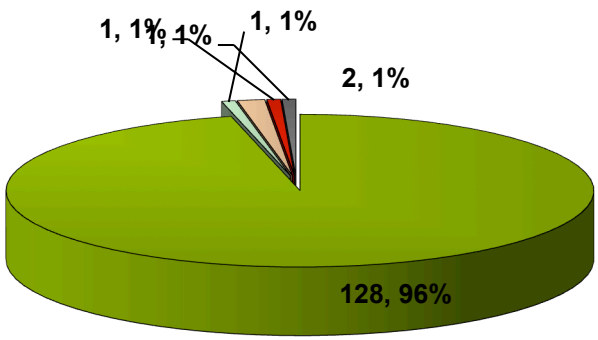
ISO 27001:2005 Standards Implementation - Status by Classification in number and percentage

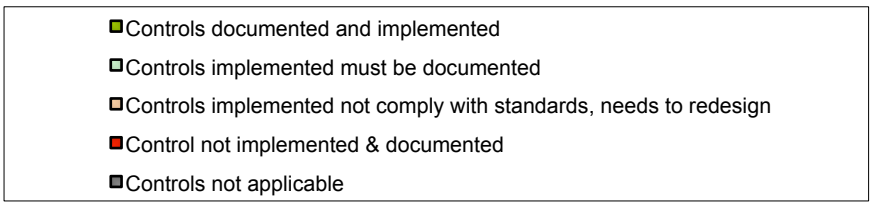


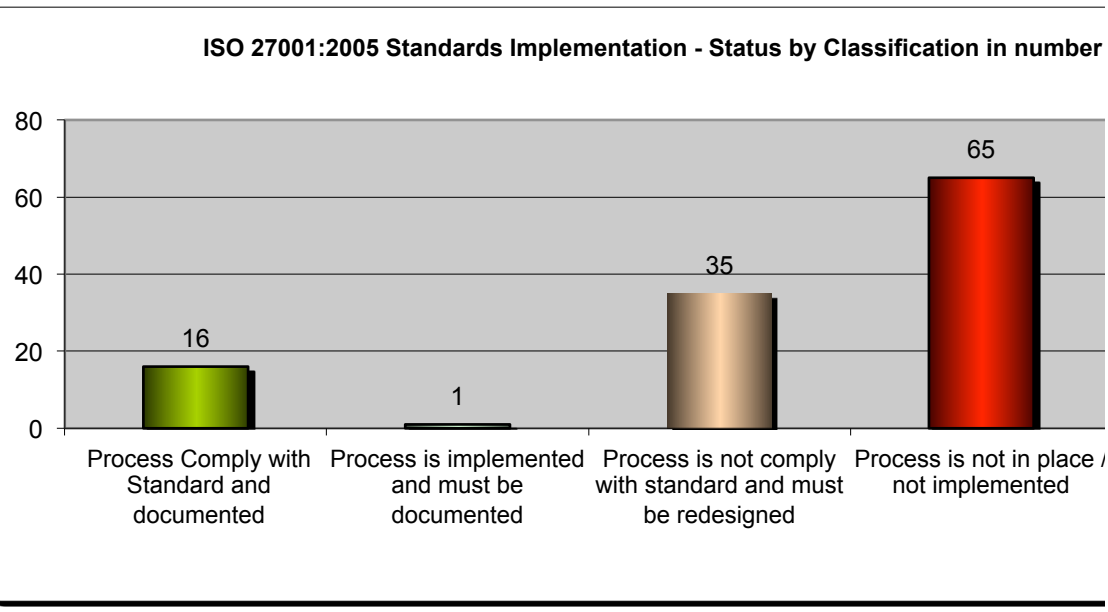
Status :- Process Implementation comply with ISO 27001:2005 standard and documented



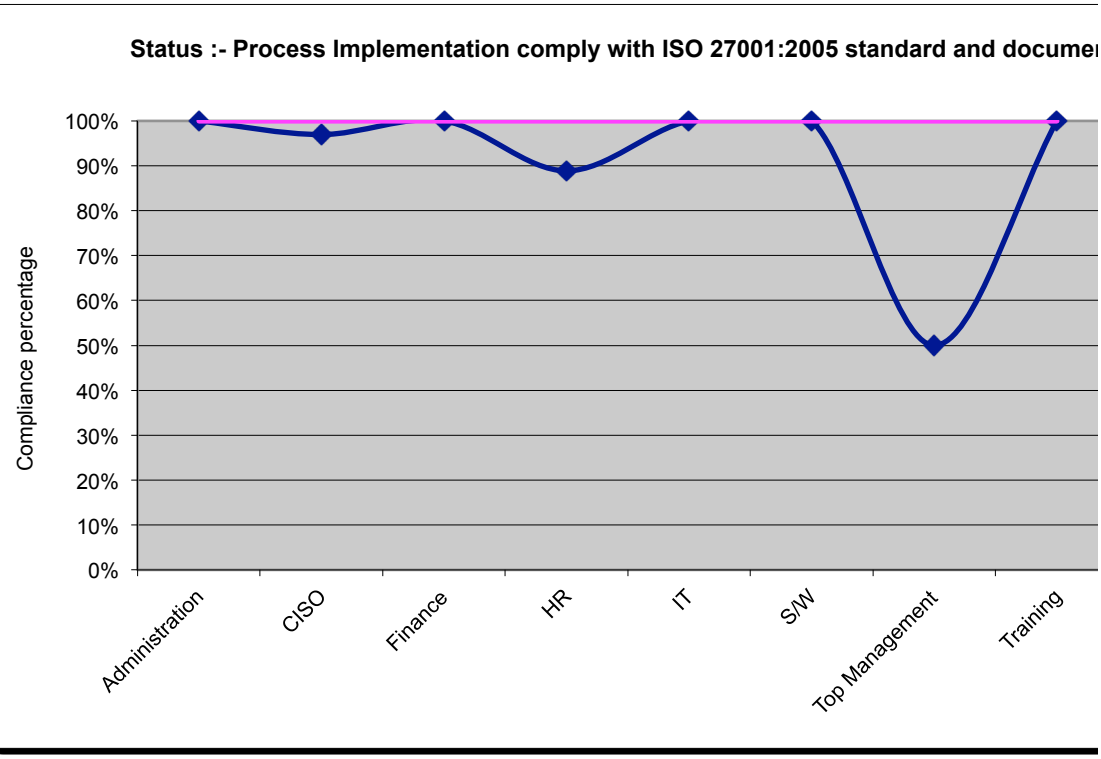
ISO 27001:2005 Annexure-A Controls Implementation Status by Classification in number and percentage

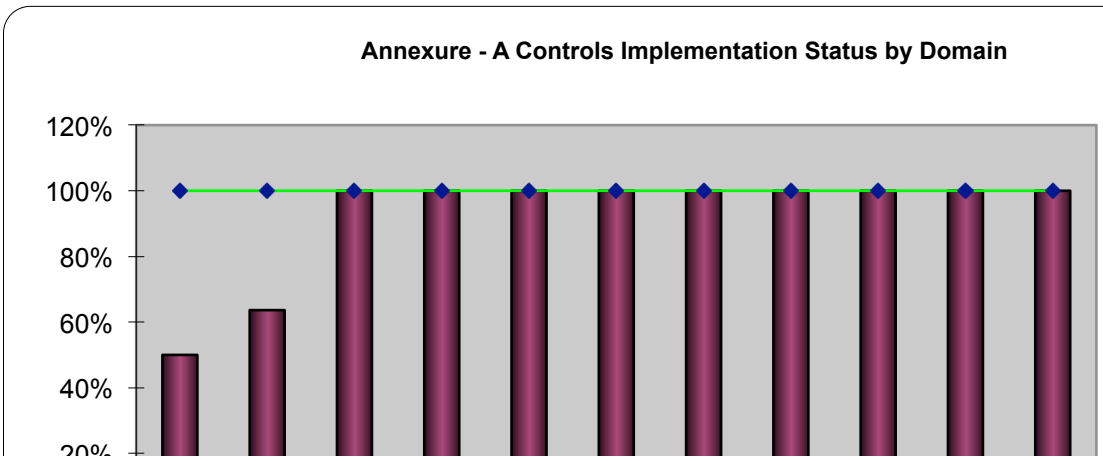



Controls documented and implemented
Controls implemented must be documented
Controls implemented not comply with standards, needs to redesign
Control not implemented & documented
Controls not applicable

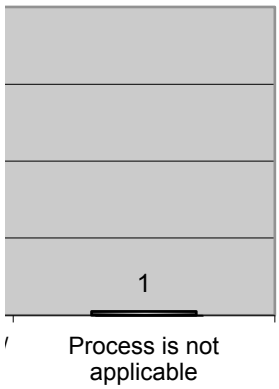

ISO 27001:2005 Standards Implementation - Status by Classification in number
80
60
40
20
0
16
1
35
65
Process Comply with Standard and documented
Process is implemented and must be documented
Process is not comply with standard and must be redesigned
Process is not in place / not implemented


action

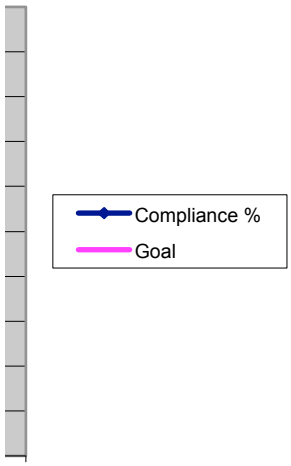

Status :- Process Implementation comply with ISO 27001:2005 standard and docume
Compliance percentage
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Administration
CISO
Finance
HR
IT
S/W
Top Management
Training

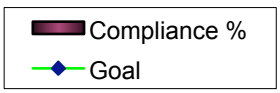

Annexure - A Controls Implementation Status by Domain
120%
100%
80%
60%
40%
20%

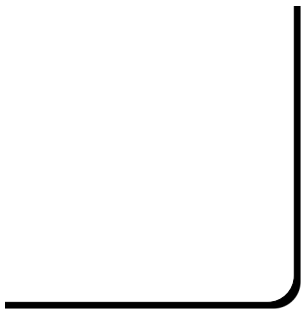
20%
0%
Security Policy
Organization of information
Asset Management
Human resources security
Physical and environmental
Communications and operations
Access Control
Information systems
Information security incident
Business continuity
Compliance


1
Process is not applicable

nted


Compliance %
Goal


Compliance %
Goal



Legend

Implementation Status by ISO 27001:2005 - Clauses			
Reference	Process Comply with Standard and documented	Process is implemented and must be documented	Process is not comply with standard and must be redesigned
ISO Clauses	16	1	35

Implementation status by ISO 27001:2005 - Annexure - A Contro			
Reference	Controls documented and implemented	Controls implemented must be documented	Controls implemented not comply with standards, needs to redesign
Controls	128	1	2

Implementation Adequacy Status against ISO 27001 Clauses		
ISO Clause	Count	Compliance %
4.1 - General Requirements	1	100%
4.2 - Establishing and managing the ISMS	5	17%
4.3 - Documentation requirements	8	31%
5.1 - Management Commitment	0	0%
5.2 - Resource Management	1	8%
6 - Internal ISMS Audit	0	0%
7.1 - General	0	0%
7.2 - Review Input	0	0%
7.3 - Review Output	0	0%
8.1 - Continual Improvement	0	0%
8.2 - Corrective action	1	14%
8.3 - Preventive action	0	0%

Implementation Adequacy Status against ISO 27001 Annexure - A Controls			
	Domain description	Count	Compliance %
5	Security Policy	1	50%
6	Organization of information security	7	64%
7	Asset Management	5	100%
8	Human resources security	9	100%
9	Physical and environmental security	13	100%
10	Communications and operations management	32	100%
11	Access Control	25	100%
12	Information systems acquisition, development and mainten	5	100%
13	Information security incident management	5	100%
14	Business continuity management	5	100%
15	Compliance	11	100%

Annexure - A Controls and Objectives - ISO 27002:2005 - Security Techniques			
Function	No. of controls	Compliance %	Goal
Administration	16	100%	100.00%
CISO	33	97%	100.00%
Finance	3	100%	100.00%
HR	9	89%	100.00%
IT	58	100%	100.00%
S/W	8	100%	100.00%
Top Management	4	50%	100.00%

Training	1	100%	100.00%

Process is not in place / not implemented	Process is not applicable
65	1

118

ls	
Control not implemented & documented	Controls not applicable
1	1

Goal
100%
100%
100%
100%
100%
100%
100%
100%
100%
100%
100%
100%

Goal
100%
100%
100%
100%
100%
100%
100%
100%
100%
100%
100%

Note :

Functions	D	PNP	RD	MD	Grand Total	Compliance %
Administration	16	0	0	0	16	100%
CISO	32	0	1	0	33	97%
Finance	3	0	0	0	3	100%
HR	8	0	0	1	9	89%
IT	58	0	0	0	58	100%
S/W	8	0	0	0	8	100%
Top Management	2	1	1	0	4	50%
Training	1	0	0	0	1	100%

Grand Total	128	1	2	1	132	

Compliance %	97%	1%	2%	1%	100%

NA	Net Total
0	
1	
0	
0	
0	
0	
0	
0	

1	133