ISO 27001 Compliance Checklist

Reference		Audit area, objective and question		Resul
Checklist	Standard	Section	Audit Question	Findings
Security Policy				
1.1	5.1	**Information Security Policy**		
1.1.1	5.1.1	Information security policy document	Whether there exists an Information security policy, which is approved by the management, published and communicated as appropriate to all employees.	
			Whether the policy states management commitment and sets out the organizational approach to managing information security.	
1.1.2	5.1.2	Review of Informational Security Policy	Whether the Information Security Policy is reviewed at planned intervals, or if significant changes occur to ensure its continuing suitability, adequacy and effectiveness.	
			Whether the Information Security policy has an owner, who has approved management responsibility for development, review and evaluation of the security policy.	
			Whether any defined Information Security Policy review procedures exist and do they include requirements for the management review.	
			Whether the results of the management review are taken into account.	
			Whether management approval is obtained for the revised policy.	
Organization of Information Security				
2.1	6.1	**Internal Organization**		
2.11	6.11	Management Commitment to Informaiton Security	Whether management demonstrates active support for security measures within the organization. This can be done via clear direction, demonstrated commitment, explicit assignment and acknowledgement of information security responsibilities.	
2.1.2	6.1.2	Information Security coordination	Whether information security activities are coordinated by representatives from diverse parts of the organization, with pertinent roles and responsibilities	

Vinod Kumar
vinodjis@hotmail.com

01/12/2011

ISO 27001 Compliance Checklist

2.1.3	6.1.3	Allocation of Information Security responsibilities	Whether responsibilities for the protection of individual assets, and for carrying out specific security processes, were clearly identified and defined.	
2.1.4	6.1.4	Authorization process for Information processing facilities	Whether management authorization process is defined and implemented for any new information processing facility within the organization.	
2.1.5	6.1.5	Confidentiality Agreements	Confidentiality or Non-Disclosure Agreement (NDA) for protection of information is clearly defined and regularly reviewed.	
			confidential information using legal enforceable terms	
2.1.6	6.1.6	Contact with Authorities	Whether there exists a procedure that describes when, and by whom: relevant authorities such as Law enforcement, fire department etc., should be contacted, and how the incident should be reported	
2.1.7	6.1.7	Contact with special interest groups	Whether appropriate contacts with special interest groups or other specialist security forums, and professional associations are maintained.	
2.1.8	6.1.8	Independent review of Information Security	Whether the organization's approach to managing information security, and its implementation, is reviewed independently at planned intervals, or when major changes to security implementation occur.	
2.2	**6.2**	**External Parties**		
2.2.1	6.2.1	Identification of risks related to external parties	Whether risks to the organization's information and information processing facility, from a process involving external party access, is identified and appropriate control measures implemented before granting access.	
2.2.2	6.2.2	Addressing security while dealing with customers	Whether all identified security requirements are fulfilled before granting customer access to the organization's information or assets.	
2.2.3	6.2.3	Addressing security in third party agreements	Whether the agreement with third parties, involving accessing, processing, communicating or managing the organization's information or information processing facility, or introducing products or services to information processing facility, complies with all appropriate security requirements.	
Asset Management				

ISO 27001 Compliance Checklist

3.1	7.1	**Responsibility for assets**		
3.1.1	7.1.1	Inventory of Assets	or register is maintained with all the important assets.	
3.1.2	7.1.2	Ownership of Assets	Whether each asset identified has an owner, a defined and agreed-upon security classification, and access restrictions that are periodically reviewed.	
3.1.3	7.1.3	Acceptable use of assets	Whether regulations for acceptable use of information and assets associated with an information processing facility were identified, documented and implemented.	
3.2	**7.2**	**Information Classification**		
3.2.1	7.2.1	Classification guidelines	Whether the information is classified in terms of its value, legal requirements, sensitivity and criticality to the organization.	
3.2.2	7.2.2	Information labelling and handling	Whether an appropriate set of procedures are defined for information labelling and handling, in accordance with the classification scheme adopted by the organization.	
Human resources security				
4.1	**8.1**	**Prior to employment**		
4.1.1	8.1.1	Roles and responsibilities	Whether employee security roles and responsibilities, contractors and third party users were defined and documented in accordance with the organization's information security policy.	
			Were the roles and responsibilities defined and clearly communicated to job candidates during the pre-employment process	
4.1.2	8.1.2	Screening	Whether background verification checks for all candidates for employment, contractors, and third party users were carried out in accordance to the relevant regulations.	
			Does the check include character reference, confirmation of claimed academic and professional qualifications and independent identity checks	
4.1.3	8.1.3	Terms and conditions of employment	Whether employee, contractors and third party users are asked to sign confidentiality or non-disclosure agreement as a part of their initial terms and conditions of the employment contract.	

ISO 27001 Compliance Checklist

			Whether this agreement covers the information security responsibility of the organization and the employee, third party users and contractors.	
4.2	**8.2**	**During Employment**		
4.2.1	8.2.1	Management Responsibilities	Whether the management requires employees, contractors and third party users to apply security in accordance with the established policies and procedures of the organization.	
4.2.2	8.2.2	Infromation security awareness, education and training	Whether all employees in the organization, and where relevant, contractors and third party users, receive appropriate security awareness training and regular updates in organizational policies and procedures as it pertains to their job function.	
4.2.3	8.2.3	Disciplinary process	Whether there is a formal disciplinary process for the employees who have committed a security breach.	
4.3	**8.3**	**Termination or change of employment**		
4.3.1	8.3.1	Termination responsibilities	Whether responsibilities for performing employment termination, or change of employment, are clearly defined and assigned.	
4.3.2	8.3.2	Return of assets	Whether there is a process in place that ensures all employees, contractors and third party users surrender all of the organization's assets in their possession upon termination of their employment, contract or agreement.	
4.3.3	8.3.3	Removal of access rights	Whether access rights of all employees, contractors and third party users, to information and information processing facilities, will be removed upon termination of their employment, contract or agreement, or will be adjusted upon change.	
Physical and Environmental security				
5.1	**9.1**	**Secure Areas**		
5.1.1	9.1.1	Physical security perimeter	Whether a physical border security facility has been implemented to protect the information processing service. Some examples of such security facilities are card control entry gates, walls, manned reception, etc	

ISO 27001 Compliance Checklist

5.1.2	9.1.2	Physical entry controls	Whether entry controls are in place to allow only authorized personnel into various areas within the organization.	
5.1.3	9.1.3	Securing offices, rooms and facilities	Whether the rooms, which have the information processing service, are locked or have lockable cabinets or safes.	
5.1.4	9.1.4	Protecting against external and enviornmental threats	Whether the physical protection against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster should be designed and applied.	
			Whether there is any potential threat from neighbouring premises.	
5.1.5	9.1.5	Working in secure areas	working in secure areas is designed and implemented	
5.1.6	9.1.6	Public access delivery and loading areas	Whether the delivery, loading, and other areas where unauthorized persons may enter the premises are controlled, and information processing facilities are isolated, to avoid unauthorized access.	
5.2	**9.2**	**Equipment Security**		
5.2.1	9.2.1	Equipment siting and protection	Whether the equipment is protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	
5.2.2	9.2.2	Supporting utilities	Whether the equipment is protected from power failures and other disruptions caused by failures in supporting utilities.	
			Whether permanence of power supplies, such as a multiple feed, an Uninterruptible Power Supply (ups), a backup generator, etc. are being utilized	
5.2.3	9.2.3	Cabling security	Whether the power and telecommunications cable, carrying data or supporting information services, is protected from interception or damage.	
			Whether there are any additional security controls in place for sensitive or critical information	
			Whether the equipment is correctly maintained to ensure its continued availability and integrity.	
			Whether the equipment is maintained, as per the supplier's recommended service intervals and specifications.	

ISO 27001 Compliance Checklist

5.2.4	9.2.4	Equipment Maintenance	Whether the maintenance is carried out only by authorized personnel.	
			Whether logs are maintained with all suspected or actual faults and all preventive and corrective measures.	
			Whether appropriate controls are implemented while sending equipment off premises. Are the equipment covered by insurance and the insurance requirements satisfied	
5.2.5	9.2.5	Securiing of equipment off-premises	Whether risks were assessed with regards to any equipment usage outside an organization's premises, and mitigation controls implemented.	
			Whether the usage of an information processing facility outside the organization has been authorized by the management.	
5.2.6	9.2.6	Secure disposal or re-use of equipment	Whether all equipment, containing storage media, is checked to ensure that any sensitive information or licensed software is physically destroyed, or securely over-written, prior to disposal or reuse.	
5.2.7	9.2.7	Removal of property	Whether any controls are in place so that equipment, information and software is not taken off-site without prior authorization.	
Communication and Operations Management				
6.1	**10.1**	**Operational procedures and responsibilites**		
6.1.1	10.1.1	Documented Operating procedures	Whether the operating procedure is documented, maintained and available to all users who need it.	
			Whether such procedures are treated as formal documents, and therefore any changes made need management authorization.	
6.1.2	10.1.2	Change Management	Whether all changes to information processing facilities and systems are controlled.	
6.1.3	10.1.3	Segregation of duties	Whether duties and areas of responsibility are separated, in order to reduce opportunities for unauthorized modification or misuse of information, or services.	

ISO 27001 Compliance Checklist

6.1.4	10.1.4	Seperation of development, test and operational facilities	Whether the development and testing facilities are isolated from operational facilities. For example, development and production software should be run on different computers. Where necessary, development and production networks should be kept separate from each other.	
6.2	**10.2**	**Third party service delivery management**		
6.2.1	10.2.1	Service delivery	Whether measures are taken to ensure that the security controls, service definitions and delivery levels, included in the third party service delivery agreement, are implemented, operated and maintained by a third party.	
6.2.2	10.2.2	Monitoring and review of third party services	Whether the services, reports and records provided by third party are regularly monitored and reviewed.	
			Whether audits are conducted on the above third party services, reports and records, on regular interval.	
6.2.3	10.2.3	Managing changes to third party services	Whether changes to provision of services, including maintaining and improving existing information security policies, procedures and controls, are managed.	
			Does this take into account criticality of business systems, processes involved and re-assessment of risks	
6.3	**10.3**	**System planning and acceptance**		
6.3.1	10.3.1	Capacity Management	Whether the capacity demands are monitored and projections of future capacity requirements are made, to ensure that adequate processing power and storage are available. Example: Monitoring hard disk space, RAM and CPU on critical servers.	
6.3.2	10.3.2	System acceptance	Whether system acceptance criteria are established for new information systems, upgrades and new versions. Whether suitable tests were carried out prior to acceptance.	
6.4	**10.4**	**Protection against malicious and mobile code**		

ISO 27001 Compliance Checklist

6.4.1	10.4.1	Controls against malicious code	Whether detection, prevention and recovery controls, to protect against malicious code and appropriate user awareness procedures, were developed and implemented	
6.4.2	10.4.2	Controls against mobile code	Whether only authorized mobile code is used. Whether the configuration ensures that authorized mobile code operates according to security policy. Whether execution of unauthorized mobile code is prevented. (Mobile code is software code that transfers from one computer to another computer and then executes automatically. It performs a specific function with little or no user intervention. Mobile code is associated with a number of middleware services.)	
6.5	**10.5**	**Backup**		
6.5.1	10.5.1	Information backup	Whether back-ups of information and software is taken and tested regularly in accordance with the agreed backup policy.	
			Whether all essential information and software can be recovered following a disaster or media failure.	
6.6	**10.6**	**Network Security Management**		
6.6.1	10.6.1	Network Controls	Whether the network is adequately managed and controlled, to protect from threats, and to maintain security for the systems and applications using the network, including the information in transit.	
			Whether controls were implemented to ensure the security of the information in networks, and the protection of the connected services from threats, such as unauthorized access.	
6.6.2	10.6.2	Security of network services	Whether security features, service levels and management requirements, of all network services, are identified and included in any network services agreement.	
			Whether the ability of the network service provider, to manage agreed services in a secure way, is determined and regularly monitored, and the right to audit is agreed upon.	
6.7	**10.7**	**Media handling**		

Vinod Kumar
vinodjis@hotmail.com

01/12/2011

ISO 27001 Compliance Checklist

6.7.1	10.7.1	Management of removable media	Whether procedures exist for management of removable media, such as tapes, disks, cassettes, memory cards, and reports.	
			Whether all procedures and authorization levels are clearly defined and documented.	
6.7.2	10.7.2	Disposal of Media	Whether the media that are no longer required are disposed of securely and safely, as per formal procedures.	
6.7.3	10.7.3	Information handling procedures	Whether a procedure exists for handling information storage.	
			Does this procedure address issues, such as information protection, from unauthorized disclosure or misuse	
6.7.4	10.7.4	Security of system documentation	Whether the system documentation is protected against unauthorized access.	
6.8	**10.8**	**Exchange of information**		
6.8.1	10.8.1	Information exchange policies and procedures	Whether there is a formal exchange policy, procedure and control in place to ensure the protection of information.	
			Does the procedure and control cover using electronic communication facilities for information exchange.	
6.8.2	10.8.2	Exchange Agreements	Whether agreements are established concerning exchange of information and software between the organization and external parties.	
			Whether the security content of the agreement reflects the sensitivity of the business information involved.	
6.8.3	10.8.3	Physical media in transit	Whether media containing information is protected against unauthorized access, misuse or corruption during transportation beyond the organization's physical boundary.	
6.8.4	10.8.4	Electronic messaging	Whether the information involved in electronic messaging is well protected. (Electronic messaging includes but is not restricted to Email, Electronic Data Interchange, Instant Messaging)	
6.8.5	10.8.5	Business Information systems	Whether policies and procedures are developed and enforced to protect information associated with the interconnection of business information systems.	

ISO 27001 Compliance Checklist

6.9	10.9	**Electronic commerce services**		
6.9.1	10.9.1	Electronic commerce	Whether the information involved in electronic commerce passing over the public network is protected from fraudulent activity, contract dispute, and any unauthorized access or modification.	
			Whether Security control such as application of cryptographic controls are taken into consideration	
			Whether electronic commerce arrangements between trading partners include a documented agreement, which commits both parties to the agreed terms of trading, including details of security issues.	
6.9.2	10.9.2	On-line transactions	Whether information involved in online transactions is protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay	
6.9.3	10.9.3	Publicly available information	Whether the integrity of the publicly available information is protected against any unauthorized modification.	
6.10	10.10	**Monitoring**		
6.10.1	10.10.1	Audit Logging	Whether audit logs recording user activities, exceptions, and information security events are produced and kept for an agreed period to assist in future investigations and access control monitoring.	
			Whether appropriate Privacy protection measures are considered in Audit log maintenance.	
6.10.2	10.10.2	Monitoring system use	Whether procedures are developed and enforced for monitoring system use for information processing facility.	
			Whether the results of the monitoring activity reviewed regularly.	
			Whether the level of monitoring required for individual information processing facility is determined by a risk assessment	
6.10.3	10.10.3	Protection of log information	well protected against tampering and unauthorized access	
6.10.4	10.10.4	Administrator and operator log	Whether system administrator and system operator activities are logged.	

6.10.4	10.10.4	Administrator and operator log	Whether the logged activities are reviewed on regular basis.	
6.10.5	10.10.5	Fault logging	Whether faults are logged analysed and appropriate action taken.	
			Whether level of logging required for individual system are determined by a risk assessment, taking performance degradation into account.	
6.10.6	10.10.6	Clock Synchronisation	Whether system clocks of all information processing system within the organization or security domain is synchronised with an agreed accurate time source. (The correct setting of computer clock is important to ensure the accuracy of audit logs)	
Access Control				
7.1	**11.1**	**Business requirement for access control**		
7.1.1	11.1.1	Access Control policy	Whether an access control policy is developed and reviewed based on the business and security requirements.	
			Whether both logical and physical access control are taken into consideration in the policy	
			Whether the users and service providers were given a clear statement of the business requirement to be met by access controls	
7.2	**11.2**	**User Access Management**		
7.2.1	11.2.1	User Registration	Whether there is any formal user registration and de-registration procedure for granting access to all information systems and services.	
7.2.2	11.2.2	Privilege Management	Whether the allocation and use of any privileges in information system environment is restricted and controlled i.e., Privileges are allocated on need-to-use basis, privileges are allocated only after formal authorization process.	
7.2.3	11.2.3	User Password Management	The allocation and reallocation of passwords should be controlled through a formal management process.	
			Whether the users are asked to sign a statement to keep the password confidential.	

ISO 27001 Compliance Checklist

7.2.4	11.2.4	Review of user access rights	Whether there exists a process to review user access rights at regular intervals. Example: Special privilege review every 3 months, normal privileges every 6 months.	
7.3	**11.3**	**User Responsibilities**		
7.3.1	11.3.1	Password use	Whether there are any security practice in place to guide users in selecting and maintaining secure passwords	
7.3.2	11.3.2	Unattended user equipment	aware of the security requirements and procedures for protecting unattended equipment. . Example: Logoff when session is finished or set up auto log off, terminate sessions when finished etc.,	
7.3.3	11.3.3	Clear desk and clear screen policy	Whether the organisation has adopted clear desk policy with regards to papers and removable storage media	
			screen policy with regards to information processing facility	
7.4	**11.4**	**Network Access Control**		
7.4.1	11.4.1	Policy on use of network services	Whether users are provided with access only to the services that they have been specifically authorized to use. Whether there exists a policy that does address	
			concerns relating to networks and network services.	
7.4.2	11.4.2	User authentication for external connections	Whether appropriate authentication mechanism is used to control access by remote users.	
7.4.3	11.4.3	Equipment identification in networks	Whether automatic equipment identification is considered as a means to authenticate connections from specific locations and equipment.	
7.4.4	11.4.4	Remote diagnostic and configuration port protection	Whether physical and logical access to diagnostic ports are securely controlled i.e., protected by a security mechanism.	
			Whether groups of information services, users and information systems are segregated on networks.	
7.4.5	11.4.5	Segregation in networks	Whether the network (where business partner's and/ or third parties need access to information system) is segregated using perimeter security mechanisms such as firewalls.	

Vinod Kumar
vinodjis@hotmail.com

01/12/2011

			Whether consideration is made to segregation of wireless networks from internal and private networks.	
7.4.6	11.4.6	Network connection control	Whether there exists an access control policy which states network connection control for shared networks, especially for those extend across organization's boundaries.	
7.4.7	11.4.7	Network routing control	Whether the access control policy states routing controls are to be implemented for networks	
			Whether the routing controls are based on the positive source and destination identification mechanism.	
7.5	**11.5**	**Operating system access control**		
7.5.1	11.5.1	Secure log-on procedures	Whether access to operating system is controlled by secure log-on procedure.	
7.5.2	11.5.2	User Identification and authentication	Whether unique identifier (user ID) is provided to every user such as operators, system administrators and all other staff including technical	
			Whether suitable authentication technique is chosen to substantiate the claimed identity of user.	
			Whether generic user accounts are supplied only under exceptional circumstances where there is a clear business benefit. Additional controls may be necessary to maintain accountability.	
7.5.3	11.5.3	Password Management system	Whether there exists a password management system that enforces various password controls such as: individual password for accountability, enforce password changes, store passwords in encrypted form, not display passwords on screen etc.,	
7.5.4	11.5.4	Use of system utilities	Whether the utility programs that might be capable of overriding system and application controls is restricted and tightly controlled.	
7.5.5	11.5.5	Session time-out	defined period of inactivity. (A limited form of timeouts can be provided for some systems, which clears the screen and prevents unauthorized access but does not close down the application or network sessions.)	

7.5.6	11.5.6	Limitation of connection time	Whether there exists restriction on connection time for high-risk applications. This type of set up should be considered for sensitive applications for which the terminals are installed in high-risk locations.	
7.6	**11.6**	**Application and Information access control**		
7.6.1	11.6.1	Information access restriction	Whether access to information and application system functions by users and support personnel is restricted in accordance with the defined access control policy.	
7.6.2	11.6.2	Sensitive system isolation	Whether sensitive systems are provided with dedicated (isolated) computing environment such as running on a dedicated computer, share resources only with trusted application systems, etc.,	
7.7	**11.7**	**Mobile computing and teleworking**		
7.7.1	11.7.1	Mobile computing and communications	Whether a formal policy is in place, and appropriate security measures are adopted to protect against the risk of using mobile computing and communication facilities.	
			Some example of Mobile computing and communications facility include: notebooks, palmtops, laptops, smart cards, mobile phones.	
			Whether risks such as working in unprotected environment is taken into account by Mobile computing policy.	
7.7.2	11.7.2		Whether policy, operational plan and procedures are developed and implemented for teleworking activities.	
		Teleworking	Whether teleworking activity is authorized and controlled by management and does it ensure that suitable arrangements are in place for this way of working.	
Information systems acquisition, development and maintenance				
8.1	**12.1**	**Security requirements of information systems**		
			Whether security requirements for new information systems and enhancement to existing information system specify the requirements for security controls.	

ISO 27001 Compliance Checklist

8.1.1	12.1.1	Security requirements analysis and specification	Whether the Security requirements and controls identified reflects the business value of information assets involved and the consequence from failure of Security.	
			Whether system requirements for information security and processes for implementing security is integrated in the early stages of information system projects.	
8.2	**12.2**	**Correct processing in applications**		
8.2.1	12.2.1	Input data validation	Whether data input to application system is validated to ensure that it is correct and appropriate.	
			Whether the controls such as: Different types of inputs to check for error messages, Procedures for responding to validation errors, defining responsibilities of all personnel involved in data input process etc., are considered.	
8.2.2	12.2.2	Control of internal processing	Whether validation checks are incorporated into applications to detect any corruption of information through processing errors or deliberate acts.	
			Whether the design and implementation of applications ensure that the risks of processing failures leading to a loss of integrity are minimised.	
8.2.3	12.2.3	Message integrity	Whether requirements for ensuring and protecting message integrity in applications are identified, and appropriate controls identified and implemented.	
			Whether an security risk assessment was carried out to determine if message integrity is required, and to identify the most appropriate method of implementation.	
8.2.4	12.2.4	Output data validation	Whether the data output of application system is validated to ensure that the processing of stored information is correct and appropriate to circumstances.	
8.3	**12.3**	**Cryptographic controls**		
			Whether the organization has Policy on use of cryptographic controls for protection of information. . Whether the policy is successfully implemented.	

ISO 27001 Compliance Checklist

8.3.1	12.3.1	Policy on use of cryptographic controls	Whether the cryptographic policy does consider the management approach towards the use of cryptographic controls, risk assessment results to identify required level of protection, key management methods and various standards for effective implementation.	
8.3.2	12.3.2	Key Management	Whether key management is in place to support the organizations use of cryptographic techniques.	
			Whether cryptographic keys are protected against modification, loss, and destruction.	
			Whether secret keys and private keys are protected against unauthorized disclosure.	
			Whether equipments used to generate, store keys are physically protected.	
			Whether the Key management system is based on agreed set of standards, procedures and secure methods.	
8.4	**12.4**	**Security of system files**		
8.4.1	12.4.1	Control of operational software	Whether there are any procedures in place to control installation of software on operational systems. (This is to minimise the risk of corruption of operational systems.)	
8.4.2	12.4.2	Protection of system test data	Whether system test data is protected and controlled. Whether use of personal information or any sensitive information for testing operational database is shunned	
8.4.3	12.4.3	Access control to program source code	Whether strict controls are in place to restrict access to program source libraries. (This is to avoid the potential for unauthorized, unintentional changes.)	
8.5	**12.5**	**Security in development and support services**		
8.5.1	12.5.1	Change control procedures	Whether there is strict control procedure in place over implementation of changes to the information system. (This is to minimise the corruption of information system.)	
			Whether this procedure addresses need for risk assessment, analysis of impacts of changes,	

ISO 27001 Compliance Checklist

8.5.2	12.5.2	Technical review of applications after operating system changes	Whether there is process or procedure in place to review and test business critical applications for adverse impact on organizational operations or security after the change to Operating Systems. Periodically it is necessary to upgrade operating system i.e., to install service packs, patches, hot fixes etc.	
8.5.3	12.5.3	Restrictions on changes to software packages	Whether modifications to software package is discouraged and/ or limited to necessary changes.	
			Whether all changes are strictly controlled.	
8.5.4	12.5.4	Information leakage	Whether controls are in place to prevent information leakage.	
			Whether controls such as scanning of outbound media, regular monitoring of personnel and system activities permitted under local legislation, monitoring resource usage are considered.	
8.5.5	12.5.5	Outsourced software development	Whether the outsourced software development is supervised and monitored by the organization.	
			Whether points such as: Licensing arrangements, escrow arrangements, contractual requirement for quality assurance, testing before installation to detect Trojan code etc., are considered.	
8.6	**12.6**	**Technical vulnerability management**		
8.6.1	12.6.1	Control of technical vulnerabilities	Whether timely information about technical vulnerabilities of information systems being used is obtained.	
			Whether the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to mitigate the associated risk.	
Information Security Incident Management				
9.1	**13.1**	**Reporting information security events and weaknesses**		
9.1.1	13.1.1	Reporting information security events	Whether information security events are reported through appropriate management channels as quickly as possible.	
			Whether formal information security event reporting procedure, Incident response and escalation procedure is developed and implemented.	

ISO 27001 Compliance Checklist

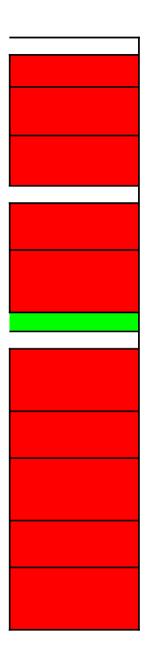|				
9.1.2	13.1.2	Reporting security weaknesses	Whether there exists a procedure that ensures all employees of information systems and services are required to note and report any observed or suspected security weakness in the system or services.	
9.2	**13.2**	**Management of information security incidents and improvements**		
9.2.1	13.2.1	Responsibilities and procedures	Whether management responsibilities and procedures were established to ensure quick, effective and orderly response to information security incidents.	
			Whether monitoring of systems, alerts and vulnerabilities are used to detect information security incidents.	
			Whether the objective of information security incident management is agreed with the management.	
9.2.2	13.2.2	Learning from information security incidents	Whether there is a mechanism in place to identify and quantify the type, volume and costs of information security incidents.	
			Whether the information gained from the evaluation of the past information security incidents are used to identify recurring or high impact incidents.	
9.2.3	13.2.3	Collection of evidence	Whether follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal).	
			Whether evidence relating to the incident are collected, retained and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).	
			Whether internal procedures are developed and followed when collecting and presenting evidence for the purpose of disciplinary action within the organization	
Business Continuity Management				
10.1	**14.1**	**Information security aspects of business continuity management**		
		Including informaiton security in the	Whether there is a managed process in place that addresses the information security requirements for developing and maintaining business continuity throughout the organization.	

10.1.1	14.1.1	Including informaiton security in the business continuity management process	Whether this process understands the risks the organization is facing, identify business critical assets, identify incident impacts, consider the implementation of additional preventative controls and documenting the business continuity plans addressing the security requirements.	
10.1.2	14.1.2	Business continuity and risk assessement	Whether events that cause interruption to business process is identified along with the probability and impact of such interruptions and their consequence for information security.	
10.1.3	14.1.3	Developing and implementing continuity plans including information security	Whether plans were developed to maintain and restore business operations, ensure availability of information within the required level in the required time frame following an interruption or failure to business processes.	
			Whether the plan considers identification and agreement of responsibilities, identification of acceptable loss, implementation of recovery and restoration procedure, documentation of procedure and regular testing.	
10.1.4	14.1.4	Business continuity planning framework	Whether there is a single framework of Business continuity plan.	
			Whether this framework is maintained to ensure that all plans are consistent and identify priorities for testing and maintenance.	
			Whether business continuity plan addresses the identified information security requirement.	
10.1.5	14.1.5	Testing maintaining and re-assessing business continuity plans	Whether Business continuity plans are tested regularly to ensure that they are up to date and effective.	
			Whether business continuity plan tests ensure that all members of the recovery team and other relevant staff are aware of the plans and their responsibility for business continuity and information security and know their role when plan is evoked.	
Compliance				
11.1	**15.1**	**Compliance with legal requirements**		

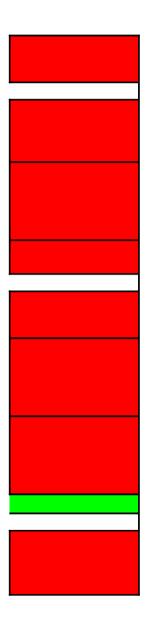# ISO 27001 Compliance Checklist

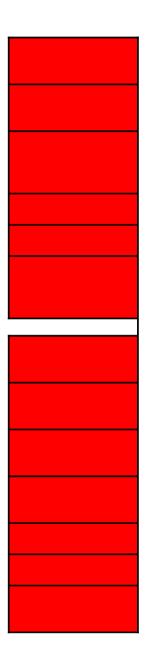|				
11.1.1	15.1.1	Identification of applicable legislation	Whether all relevant statutory, regulatory, contractual requirements and organizational approach to meet the requirements were explicitly defined and documented for each information system and organization.	
			Whether specific controls and individual responsibilities to meet these requirements were defined and documented.	
11.1.2	15.1.2	Intellectual property rights (IPR)	Whether there are procedures 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.	
			Whether the procedures are well implemented.	
			Whether controls such as: publishing intellectual property rights compliance policy, procedures for acquiring software, policy awareness, maintaining proof of ownership, complying with software terms and conditions are considered.	
11.1.3	15.1.3	Protection of organizational records	Whether important records of the organization is protected from loss destruction and falsification, in accordance with statutory, regulatory, contractual and business requirement.	
			Whether consideration is given to possibility of deterioration of media used for storage of records.	
			Whether data storage systems were chosen so that required data can be retrieved in an acceptable timeframe and format, depending on requirements to be fulfilled.	
11.1.4	15.1.4	Data protection and privacy of personal information	Whether data protection and privacy is ensured as per relevant legislation, regulations and if applicable as per the contractual clauses.	
			Whether use of information processing facilities for any non-business or unauthorized purpose, without management approval is treated as improper use of the facility.	

ISO 27001 Compliance Checklist

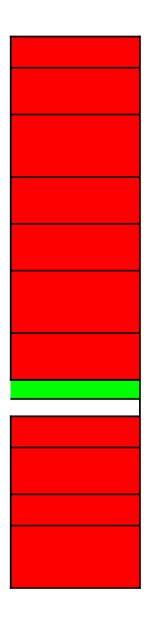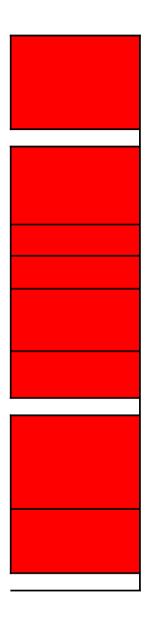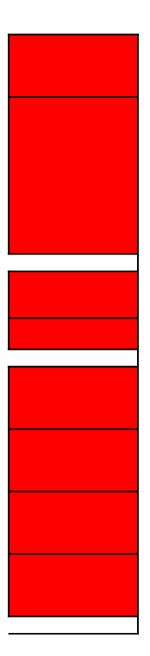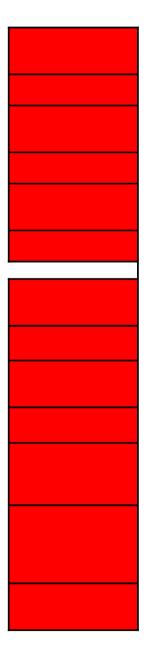|				
11.1.5	15.1.5	Prevention of misuse of information processing facilities	Whether a log-on a warning message is presented on the computer screen prior to log-on. Whether the user has to acknowledge the warning and react appropriately to the message on the screen to continue with the log-on process.	
			Whether legal advice is taken before implementing any monitoring procedures.	
11.1.6	15.1.6	Regulation of cryptographic controls	Whether the cryptographic controls are used in compliance with all relevant agreements, laws, and regulations.	
11.2	**15.2**	**Compliance with techincal policies and standards and technical compliance**		
11.2.1	15.2.1	Compliance with security policies and standards	Whether managers ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.	
			Do managers regularly review the compliance of information processing facility within their area of responsibility for compliance with appropriate security policy and procedure	
11.2.2	15.2.2	Technical compliance checking	Whether information systems are regularly checked for compliance with security implementation standards.	
			Whether the technical compliance check is carried out by, or under the supervision of, competent, authorized personnel	
11.3	**15.3**	**Information systems audit considerations**		
11.3.1	15.3.1	Information systems audit control	Whether audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimise the risk of disruptions to business process.	
			Whether the audit requirements, scope are agreed with appropriate management.	
11.3.2	15.3.2	Protection of informaiton system audit tools	Whether access to information system audit tools such as software or data files are protected to prevent any possible misuse or compromise. Whether information system audit tools are separated from development and operational systems, unless given an appropriate level of additional protection.	

ISO 27001 Compliance Checklist

ts
Status (%)

Vinod Kumar
vinodjis@hotmail.com

01/12/2011

ISO 27001 Compliance Checklist

ISO 27001 Compliance Checklist

Vinod Kumar
vinodjis@hotmail.com

01/12/2011

ISO 27001 Compliance Checklist

Vinod Kumar
vinodjis@hotmail.com

01/12/2011

ISO 27001 Compliance Checklist

Vinod Kumar
vinodjis@hotmail.com

01/12/2011

ISO 27001 Compliance Checklist

Vinod Kumar
vinodjis@hotmail.com

01/12/2011

ISO 27001 Compliance Checklist

ISO 27001 Compliance Checklist

ISO 27001 Compliance Checklist

Vinod Kumar
vinodjis@hotmail.com

01/12/2011

ISO 27001 Compliance Checklist

Vinod Kumar
vinodjis@hotmail.com

01/12/2011

ISO 27001 Compliance Checklist

ISO 27001 Compliance Checklist

ISO 27001 Compliance Checklist

Vinod Kumar
vinodjis@hotmail.com

01/12/2011

ISO 27001 Compliance Checklist

ISO 27001 Compliance Checklist

ISO 27001 Compliance Checklist

Vinod Kumar
vinodjis@hotmail.com

01/12/2011

ISO 27001 Compliance Checklist

Vinod Kumar
vinodjis@hotmail.com

01/12/2011

ISO 27001 Compliance Checklist

ISO 27001 Compliance Checklist

Domain	Objectives	Status (%)
Security Policy	Information Security Policy	0%
Organization of Information Security	Internal Organization	0%
	External Parties	0%
Asset Management	Responsibilities for assets	0%
	Information Classification	0%
Human resources security	Prior to Employment	0%
	During Employment	0%
	Termination or change of employment	0%
Physical and Enviornmental security	Secure Areas	0%
	Equipment Security	0%
Communication and Operations Management	Operational procedures and responsibilities	0%
	Third party service delivery management	0%
	System planning and acceptance	0%
	Protection against malicious and mobile code	0%
	Backup	0%
	Network Security Management	0%
	Media handling	0%
	Exchange of information	0%
	Electronic commerce services	0%
	Monitoring	0%
Access Control	Business Control for access control	0%
	User Access Management	0%
	User Responsibilities	0%
	Network Access control	0%
	Operating system access control	0%
	Application and information access control	0%
	Mobile computing and teleworking	0%
rmation system acquisition, development and maintane	Security requirements of information systems	0%
	Correct processing in applications	0%
	Cryptographic controls	0%
	Security of system files	0%
	Security in development and support services	0%
	Technical vulnerability management	0%
Information security incident management	Reporting information security events and weaknesses	0%
	Management of information security incidents and imporvements	0%
Business Continuity Management	Information security aspects of Business continuity management	0%
Compliance	Compliance with legal requirements	0%
	Complinace with techinal policies and standards and technical complin	0%
	Information system audit considerations	0%

ISO 27001 Compliance Checklist

Domain	Status (%)
Security Policy	0%
Organization of Information Security	0%
Asset Management	0%
Human resources security	0%
Physical and Enviornmental security	0%
Communication and Operations Management	0%
Access Control	0%
Information system acquisition, development and main	0%
Information security incident management	0%
Business Continuity Management	0%
Compliance	0%

Compliance per Domain

Status

100%	
90%	
80%	
70%	
60%	
50%	
40%	
30%	
20%	
10%	
0%	

0% 0% 0% 0% 0% 0% 0% 0% 0% 0% 0%

Security Policy

Organization of Information Security

Asset Management

Human resources security

Physical and Enviornmental security

Communication and Operations Management

Access Control

nation system acquisition, development and maintanence

Information security incident management

Business Continuity Management

Compliance

Domain

ISO 27001 Compliance Checklist

Compliance Checklist

A conditional formatting has been provided on "Compliance checklist" sheet under the

1 to 25	
26 to 75	
76 to 100	

In the field "Findings" fill in the evidence that you saw and your thoughts of the imple
In the field "Status (%)" fill in the compliance level on the scale as mentioned above
If any of the controls in not applicable, please put in "NA" or anything that denotes tha

Compliance Per Control

Kindly note: this sheet has been automated and will show you the status pertaining to
per your status in the "Complinace Checklist" sheet

Compliance Per Domain

Kindly note: this sheet has been automated and will show you the status pertaining to
status in the "Complinace Checklist" sheet

Graphical Representation

This will give you a graphical representation of the status per domain. Which can be i

e "Status (%)" filed and is as mentioned

mentation

at particular control is not applicable to the organiz

ɔ each control objective, as

ɔ each domain, as per your

n-corporated into your presentation to the manage