ISO 27002 Audit

Auditor Name:Tata Consultancy Services
Date:2013-10-24

ISO 27002 Audit

Location Name:Italy Date:2013-10-24

Company Name:Tata Consultancy Services Auditor Name:parag

Section	Title	Requirement	Conformance	Comments/Observation
6.1	Internal Organization	6.1.1 Management commitment to information security Management should demonstrate active support for security measures within the organization. This can be done via clear direction, demonstrated commitment, explicit assignment and acknowledgement of infor	Minor	
		6.1.2 Information security coordination In a large organization it might be necessary to coordinate information security measures through a cross- functional forum.	Minor	
		6.1.3 Allocation of information security responsibilities Responsibilities for the protection of individual assets and for carrying out specific security processes should be explicitly defined. This objective includes virus protection.	YES	
		6.1.4 Authorization process for IT facilities Installation of IT facilities should be technically approved and authorized.	YES	
		6.1.5 Confidentiality agreements The organization's need for Confidentiality or Non-Disclosure Agreement (NDA) for protection of information should be clearly defined and regularly reviewed.	YES	
		6.1.6 Contact with authorities The organization should have 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.	YES	
		6.1.7 Contact with special interest groups The organization should maintain appropriate contacts with special interest groups or other specialist security forums, and professional associations.	YES	
		6.1.8 Independent review of information security The organization's approach to managing information security, and its implementation, should be reviewed independently at planned intervals, or when major changes to security implementation occur.	YES	
7.1	Responsibility of Assets	7.1.1 Inventory of assets Inventories should be maintained of all major information and IT assets.	YES	
		7.1.2 Ownership of assets Each asset identified should have an owner, a defined and agreed-upon security classification, and access restrictions that are periodically reviewed.	YES	
		7.1.3 Acceptable use of assets Regulations for acceptable use of information and assets associated with an information processing facility should be identified, documented and implemented.	YES	
7.2	Information classification	7.2.1 Classification guidelines Protection for classified information should be consistent with business needs.	YES	

ISO 27002 Audit

Location Name:Italy Date:2013-10-24

Company Name:Tata Consultancy Services Auditor Name:parag

		7.2.2 Information labeling and handling Classified information and outputs from systems handling organizationally classified data should be labeled appropriately.	YES	
8.1	Prior to employment	8.1.1 Security in job descriptions	YES	
		8.1.2 Recruitment screening	YES	
		8.1.3 Terms and conditions of employment	YES	
8.2	During employment	8.2.1 Management responsibilities Management should require employees, contractors and third party users to apply security in accordance with the established policies and procedures of the organization.	YES	
		8.2.2 Information security awareness, education and training All employees in the organization, and where relevant, contractors and third party users, should receive appropriate security awareness training and regular updates in organizational policies an	YES	
		8.2.3 Disciplinary process A disciplinary process is essential for dealing with security breaches.	YES	
8.3	Termination or change of employment	8.3.1 Termination responsibilities Responsibilities for performing employment termination, or change of employment, should be clearly defined and assigned.	YES	
		8.3.2 Return of assets The organization should have 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 agreemen	YES	
		8.3.3 Removal of access rights Access rights of all employees, contractors and third party users, to information and information processing facilities, should be removed upon termination of their employment, contract or agreement, or will be adjusted upo	YES	
9.1	Secure areas	9.1.1 Physical security perimeter Physical security protection should be based on defined perimeters.	YES	
		9.1.2 Physical entry controls Secure areas should be protected by appropriate entry controls.	YES	
		9.1.3 Securing Offices, rooms and facilities Data centers and computer rooms supporting critical business activities should have good physical security.	YES	
		9.1.4 Protecting against external and environment threats 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.	YES	

ISO 27002 Audit

Location Name:Italy Date:2013-10-24

Company Name:Tata Consultancy Services Auditor Name:parag

		9.1.5 Working in Secure Areas Information should be provided only on a need to know basis. There should be security controls in place for third parties or personnel working in secure areas.	YES	
		9.1.6 Isolated delivery loading areas An intermediate holding area should be considered for deliveries to computer rooms. A risk assessment should be used to determine the security required in delivery and loading areas.	YES	
9.2	Equipment security	9.2.1 Equipment siting and protection Equipment should be sited or protected to reduce the risks of damage, interference and unauthorized access.	YES	
		9.2.2 Power supplies Equipment should be protected from power failures or other electrical anomalies.	YES	
		9.2.3 Cabling security Power and telecommunication cabling should be protected from interception or damage.	YES	
		9.2.4 Equipment maintenance Equipment should be appropriately maintained. Logs should be maintained with all suspected or actual faults and all preventive and corrective measures. Controls should be in place for equipment sent off-site.	YES	
		9.2.5 Security of equipment off- premises Security procedures and controls should cover the security of equipment used outside an organization's premises. The controls in place for the equipment should meet or exceed the security provided inside the premi	YES	
		9.2.6 Secure disposal or re-use of equipment Data should be physically destroyed or securely over written.	YES	
10.1	Operational procedures and responsibilities	10.1.1 Documented operating procedures Documented procedures should be provided for the operation of all computer systems.	YES	
		10.1.2 Operational Change Control All programs running on production systems should be subject to strict change control. All changes made to production programs should be logged.	YES	
		10.1.3 Incident management procedures Incident management responsibilities and procedures should be established.	YES	
		10.1.4 Segregation of duties Segregation of duties minimizes the risk of negligent or deliberate system misuse.	YES	
		10.1.5 Separation of development and operational facilities Development and testing facilities should be isolated from operational systems.	YES	

ISO 27002 Audit

Location Name:Italy Date:2013-10-24

Company Name:Tata Consultancy Services Auditor Name:parag

10.2	Third party service delivery management	10.2.2 Monitoring and review of third party services The services, reports and records provided by third party should be regularly monitored and reviewed. Audits should be conducted on the above third party services, reports and records, on regular interv	YES	
		10.2.3 Managing changes to third party services Changes to provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed.	YES	
10.3	System Planning and Acceptance	10.3.1 Capacity planning Capacity requirements should be monitored to avoid failures due to inadequate capacity.	YES	
		10.3.2 System acceptance Acceptance criteria for new systems should be established and suitable tests carried out prior to acceptance.	YES	
10.4	Protection from malicious software	10.4.1 Control against malicious code Virus detection and prevention measures and appropriate user awareness procedures should be implemented.	YES	
		10.4.2 Control against mobile code Only authorized mobile code should be used. The configuration should ensure that authorized mobile code operates according to security policy. Execution of unauthorized mobile code should be prevented.	YES	
10.5	Backup	10.5.1 Data back-up Back-up copies of essential business data and software should be regularly taken. Backups should be stored securely well away from the actual site. Backup media should be regularly tested.	YES	
10.6	Network security management	10.6.1 Network security controls A range of security controls is required in computer networks.	YES	
		10.6.2 Security of network services The risks associated with the use of network services should be established.	YES	
10.7	Media handling	10.7.1 Management of removable computer media Removable computer media should be controlled.	YES	
		10.7.2 Disposal of media Media should be disposed of securely and safely when no longer required. Sensitive information could be leaked to outside persons through careless disposal of media. Formal procedures for the secure disposal of media should be es	YES	
		10.7.3 Information handling procedures Procedures for handling sensitive data should be established.	YES	
		10.7.4 Security of system documentation System documentation should be protected from unauthorized access.	YES	
10.8	Exchange of information	10.8.1 Information exchange policies and procedures Procedures and controls should be in place to protect the exchange of information through the use of voice, facsimile and video communications facilities.	YES	

ISO 27002 Audit

Location Name:Italy Date:2013-10-24

Company Name:Tata Consultancy Services Auditor Name:parag

		10.8.2 Information and software exchange agreements Agreements for the exchange of data and software should specify security controls.	YES	
		10.8.3 Security of media in transit Computer media in transit should be protected from loss or misuse.	YES	
		10.8.4 Electronic Messaging Whether the information involved in electronic messaging should be well protected. (Electronic messaging includes but is not restricted to Email, Electronic Data Interchange, Instant Messaging)	YES	
		10.8.5 Business information systems Clear policies and guidelines are required to control the business and security risks associated with electronic office systems.	YES	
10.9	Electronic commerce services	10.9.1 Electronic Commerce security Special security controls should be applied where necessary to protect electronic commerce	YES	
		10.9.2 On-Line Transactions Information involved in online transactions should be protected to prevent incomplete transmission, mis- routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	YES	
		10.9.3 Publicly available systems Care should be taken to protect the integrity of electronically published information to prevent unauthorized modification which could harm the reputation of the publishing organization. Information on a publicly availab	YES	
10.10	Monitoring	10.10.1 Audit logging Audit trails of security events should be maintained.	YES	
		10.10.2 Monitoring system use Procedures for monitoring system use should be established.	YES	
		10.10.3 Protection of log information The Logging facility and log information should be well protected against tampering and unauthorized access.	YES	
		10.10.4 Administrator and Operator logs Computer operators should maintain a log of all work carried out.	YES	
		10.10.5 Fault logging Faults should be reported and corrective action taken.	YES	
		10.10.6 Clock synchronization Computer clocks should be synchronized for accurate recording.	YES	
11.1	Business requirement for system access	11.1.1 Documented access control policy Business requirements for access control should be defined and documented.	YES	
11.2	User access management	11.2.1 User registration There should be a formal user registration and de-registration procedure for access to all multi-user IT services.	YES	
		11.2.2 Privilege management The use of special privileges should be restricted and controlled.	YES	

ISO 27002 Audit

Location Name:Italy Date:2013-10-24

Company Name:Tata Consultancy Services Auditor Name:parag

		11.2.3 User password management The allocation of user passwords should be securely controlled.	YES	
		11.2.4 Review of user access rights. User access rights should be reviewed at regular intervals.	YES	
11.3	User responsibilities	11.3.1 Password use Users should follow good security practices in the selection and use of passwords.	YES	
		11.3.2 Unattended user equipment Users should ensure that unattended equipment has appropriate security protection.	YES	
		11.3.3 Clear Desk and clear screen policy An automatic computer screen locking facility should be enabled. Employees should be advised to leave any confidential material in the form of paper documents, media etc., only in suitable locked container while	YES	
11.4	Network access control	11.4.1 Policy on use of network services Users should only be able to gain access to the services that they are authorized to use.	YES	
		11.4.2 User authentication for external connections Connections by remote users via public (or non-organization) networks should be authenticated.	YES	
		11.4.3 Equipment identification in networks Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.	YES	
		11.4.4 Remote diagnostic and configuration port protection Access to diagnostic ports should be securely controlled.	YES	
		11.4.5 Segregation in networks Large networks may have to be divided into separate domains.	YES	
		11.4.6 Network connection control The connection capability of users may need to be controlled to support the access policy requirements of certain business applications.	YES	
		11.4.7 Network routing control Shared networks may require network routing controls.	YES	
11.5	Computer system access control	11.5.1 Secure logon procedures Access to IT services should be via a secure logon process.	YES	
		11.5.2 User identification and authentication Computer activities should be traceable to individuals.	YES	
		11.5.3 Password management system An effective password system should be used to authenticate users.	YES	
		11.5.4 Use of system utilities Most computer installations have one or more system utility programs that might be capable of overriding system and application controls. It is essential that their use is restricted and tightly controlled.	YES	

ISO 27002 Audit

Location Name:Italy | Date:2013-10-24

Company Name:Tata Consultancy Services | Auditor Name:parag

		11.5.5 Session time-out Inactive terminals in high risk locations, or serving high risk systems, should be set to time out, to prevent access by unauthorized persons.	YES	
		11.5.6 Limitation of connection time Restrictions on connection times should provide additional security for high-risk applications.	YES	
11.6	Application and information access control	11.6.1 Information access restriction Access to data and IT services should be granted in accordance with business access policy.	YES	
		11.6.2 Sensitive system isolation Sensitive systems might require a dedicated (isolated) computing environment.	YES	
11.7	Mobile computing and teleworking	11.7.1 Mobile Computing and communications When using mobile computing facilities, e.g. notebooks, palmtops, laptops and mobile phones, special care should be taken to ensure that business information is not compromised.	YES	
		11.7.2 Teleworking Suitable protection of the teleworking site should be in place against, e.g., the theft of equipment and information, the unauthorized disclosure of information, unauthorized remote access to the organization's internal systems or misu	YES	
12.1	Security requirements of information systems	12.1.1 Security requirements analysis and specification An analysis of security requirements should be carried out at the requirements analysis stage of each development project.	YES	
12.2	Correct processing in applications	12.2.1 Input data validation Data input to application systems should be validated.	YES	
		12.2.2 Control of internal processing Data that has been correctly entered can be corrupted by processing errors or through deliberate acts. Validation checks should be incorporated into systems to detect such corruption. The design of applications shoul	YES	
		12.2.3 Message integrity Requirements for ensuring and protecting message integrity in applications should be identified, and appropriate controls identified and implemented.	YES	
		12.2.4 Output data validation Data output from an application system should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances	YES	
12.3	Cryptographic controls	12.3.1 Policy on the use of cryptographic controls There should be a Policy in place regarding use of cryptographic controls for protection of information.	YES	
		12.3.2 Key management Whether there is a management system is in place to support the organization's use of cryptographic techniques such as Secret key technique and Public key technique.	YES	

ISO 27002 Audit

Location Name:Italy Date:2013-10-24

Company Name:Tata Consultancy Services Auditor Name:parag

12.4	Security of system files	12.4.1 Control of operational software There should be formal change control procedures.	YES	
		12.4.2 Protection of system test data System test data should be protected and controlled. The use of operational database containing personal information should be avoided for test purposes.	YES	
		12.4.3 Access control to program source library There should be strict controls in place over access to program source libraries. This is to reduce the potential for corruption of computer programs.	YES	
12.5	Security in development and support process	12.5.1 Access control to program source library The organization should have strict control procedures in place over implementation of changes to the information system. (This is to minimize the corruption of the information system).	YES	
		12.5.2 Technical review of applications after operating system changes The organization should have a process or procedure in place to review and test business critical applications for adverse impact on organizational operations or security after the cha	YES	
		12.5.3 Access control to program source library All modifications to software packages are discouraged and/ or limited to necessary changes.	YES	
		12.5.4 Information leakage The organization should have controls in place to prevent information leakage.	YES	
12.6	Technical Vulnerability Management	12.6.1 Control of technical vulnerabilities Timely information about technical vulnerabilities of information systems being used should be obtained. The organization's exposure to such vulnerabilities should be evaluated and appropriate measures taken to	YES	
13.1	Security in development and support process	13.3.1 Reporting of security incidents Security incidents should be reported through management channels as quickly as possible.	YES	
		13.3.2 Reporting of security weaknesses Suspected security weaknesses should be reported.	YES	
13.2	Management of information security incidents and improvements	13.2.1 Responsibilities and procedures Incident management responsibilities and procedures should be established.	YES	
		13.2.2 Learning from security incidents There should be mechanisms in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored.	YES	
		13.2.3 Collection of evidence Follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal).	YES	

ISO 27002 Audit

Location Name:Italy Date:2013-10-24

Company Name:Tata Consultancy Services Auditor Name:parag

14.1	Aspects of business continuity planning	14.1.1 Including information security in the business continuity management process There should be a managed process in place for developing and maintaining business continuity plans across the organization.	YES	
		14.1.2 Business continuity and risk assessment A consistent framework of business continuity plans should be maintained.	YES	
		14.1.3 Developing and implementing continuity plans including information security Plans should be developed to maintain and restore business operations, ensure availability of information within the required level in the required time frame following an	YES	
		14.1.4 Business continuity planning framework The organization should have a single framework for the Business continuity plan.	YES	
		14.1.5 Business continuity and risk assessment The organization should have a single framework for the Business continuity plan.	YES	
15.1	Compliance with legal requirements	15.1.1 Identification of applicable legislation All relevant statutory, regulatory, contractual requirements and organizational approach to meet the requirements should be explicitly defined and documented for each information system and organization.	YES	
		15.1.2 Intellectual property rights (IPR) The organization should have 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 th	YES	
		15.1.3 Protection of organizational records Important records of an organization should be protected from loss, destruction and falsification.	YES	
		15.1.4 Data protection and privacy of personal information Applications handling personal data on individuals should comply with data protection legislation and principles.	YES	
		15.1.5 Prevention of misuse of information processing facility IT facilities should only be used for authorized business purposes.	YES	
		15.1.6 Regulation of cryptographic controls Cryptographic controls should used in compliance with all relevant agreements, laws, and regulations.	YES	
15.2	Compliance with security policies and standards, and technical compliance	15.2.1 Compliance with security policy and standards All areas within the organization should be considered for regular review to ensure compliance with security policies and standards.	Major	
		15.2.2 Technical compliance checking IT facilities should be regularly checked for compliance with security implementation standards.	Major	

ISO 27002 Audit

Location Name:Italy

Date:2013-10-24

Company Name:Tata Consultancy Services

Auditor Name:parag

15.3	Information System audit considerations	15.3.1 Information systems audit controls Audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruptions to business process.	YES	
		15.3.2 Protection of information system audit tools Access to information system audit tools such as software or data files should be protected to prevent any possible misuse or compromise.	Minor	dsfdsfdfdfddff

Recommendation

fdgggfgfgfdgfdgfd