



Interested in learning more
about security
management?

SANS Institute

Security Consensus Operational Readiness Evaluation

This checklist is from the SCORE Checklist Project. Reposting is not permitted without express, written permission.

ISO 17799 Checklist

Information Security Management

BS 7799.2:2002

Audit Check List

for SANS

Author: Val Thiagarajan B.E., M.Comp, CCSE, MCSE, SPS (FW), IT Security Consultant.

Approved by: Algis Kibirktis

Owner: SANS

Extracts from BS 7799 part 1: 1999 are reproduced with the permission of BSI under license number 2003DH0251. British Standards can be purchased from BSI Customer Services, 389 Chiswick High Road, London W4 4AL. Tel : 44 (0)20 8996 9001. email: customerservices@bsi-global.com

Table of Contents

Security Policy	9
Information security policy.....	9
Information security policy document	9
Review and evaluation.....	9
Organisational Security	10
Information security infrastructure	10
Management information security forum	10
Information security coordination.....	10
Allocation of information security responsibilities.....	10
Authorisation process for information processing facilities	10
Specialist information security advise	11
Co-operation between organisations	11
Independent review of information security	11
Security of third party access.....	11
Identification of risks from third party access	11
Security requirements in third party contracts	12
Outsourcing.....	12
Security requirements in outsourcing contracts	12
Asset classification and control	12
Accountability of assets	12
Inventory of assets	12
Information classification.....	12
Classification guidelines	12
Information labelling and handling.....	12

Personnel security	12
Security in job definition and Resourcing	12
Including security in job responsibilities	12
Personnel screening and policy.....	12
Confidentiality agreements	12
Terms and conditions of employment	12
User training.....	12
Information security education and training	12
Responding to security incidents and malfunctions	12
Reporting security incidents.....	12
Reporting security weaknesses	12
Reporting software malfunctions	12
Learning from incidents.....	12
Disciplinary process	12
Physical and Environmental Security	12
Secure Area	12
Physical Security Perimeter	12
Physical entry Controls	12
Securing Offices, rooms and facilities	12
Working in Secure Areas	12
Isolated delivery and loading areas	12
Equipment Security.....	12
Equipment siting protection.....	12
Power Supplies.....	12
Cabling Security.....	12
Equipment Maintenance	12
Securing of equipment off-premises.....	12
Secure disposal or re-use of equipment	12
General Controls	12

BS 7799 Audit Checklist
6/08/2003

Clear Desk and clear screen policy..... 12
Removal of property 12

Communications and Operations Management 12

Operational Procedure and responsibilities 12
 Documented Operating procedures..... 12
 Operational Change Control 12
 Incident management procedures..... 12
 Segregation of duties..... 12
 Separation of development and operational facilities..... 12
 External facilities management 12
System planning and acceptance..... 12
 Capacity Planning 12
 System acceptance 12
Protection against malicious software 12
 Control against malicious software..... 12
Housekeeping..... 12
 Information back-up..... 12
 Operator logs..... 12
 Fault Logging..... 12
Network Management..... 12
 Network Controls 12
Media handling and Security 12
 Management of removable computer media..... 12
 Disposal of Media 12
 Information handling procedures..... 12
 Security of system documentation..... 12
Exchange of Information and software 12
 Information and software exchange agreement 12
 Security of Media in transit..... 12

BS 7799 Audit Checklist
6/08/2003

Electronic Commerce security..... 12
Security of Electronic email..... 12
Security of Electronic office systems 12
Publicly available systems 12
Other forms of information exchange 12

Access Control **12**

Business Requirements for Access Control..... 12
 Access Control Policy..... 12
User Access Management 12
 User Registration..... 12
 Privilege Management 12
 User Password Management 12
 Review of user access rights 12
User Responsibilities 12
 Password use 12
 Unattended user equipment 12
Network Access Control..... 12
 Policy on use of network services..... 12
 Enforced path..... 12
 User authentication for external connections..... 12
 Node Authentication..... 12
 Remote diagnostic port protection..... 12
 Segregation in networks..... 12
 Network connection protocols 12
 Network routing control..... 12
 Security of network services..... 12
Operating system access control..... 12
 Automatic terminal identification..... 12
 Terminal log-on procedures..... 12

BS 7799 Audit Checklist
6/08/2003

User identification and authorisation.....	12
Password management system.....	12
Use of system utilities.....	12
Duress alarm to safeguard users.....	12
Terminal time-out	12
Limitation of connection time.....	12
Application Access Control	12
Information access restriction.....	12
Sensitive system isolation.....	12
Monitoring system access and use	12
Event logging.....	12
Monitoring system use	12
Clock synchronisation.....	12
Mobile computing and teleworking	12
Mobile computing	12
Teleworking	12
System development and maintenance	12
Security requirements of systems	12
Security requirements analysis and specification	12
Security in application systems.....	12
Input data validation.....	12
Control of internal processing.....	12
Message authentication.....	12
Output data validation.....	12
Cryptographic controls.....	12
Policy on use of cryptographic controls.....	12
Encryption.....	12
Digital Signatures.....	12
Non-repudiation services	12

BS 7799 Audit Checklist
6/08/2003

Key management 12
Security of system files 12
 Control of operational software 12
 Protection of system test data 12
 Access Control to program source library 12
Security in development and support process 12
 Change control procedures 12
 Technical review of operating system changes 12
 Technical review of operating system changes 12
 Covert channels and Trojan code 12
 Outsourced software development 12

Business Continuity Management 12

Aspects of Business Continuity Management 12
 Business continuity management process 12
 Business continuity and impact analysis 12
 Writing and implementing continuity plan 12
 Business continuity planning framework 12
 Testing, maintaining and re-assessing business continuity plan 12

Compliance 12

Compliance with legal requirements 12
 Identification of applicable legislation 12
 Intellectual property rights (IPR) 12
 Safeguarding of organisational records 12
 Data protection and privacy of personal information 12
 Prevention of misuse of information processing facility 12
 Regulation of cryptographic controls 12
 Collection of evidence 12
Reviews of Security Policy and technical compliance 12

BS 7799 Audit Checklist

6/08/2003

Compliance with security policy 12
Technical compliance checking 12
System audit considerations 12
System audit controls 12
Protection of system audit tools 12

References **12**

Audit Checklist

Auditor Name: _____

Audit Date: _____

Information Security Management BS 7799.2:2002 Audit Check List						
Reference		Audit area, objective and question			Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance	
Security Policy						
1.1	3.1	<i>Information security policy</i>				
1.1.1	3.1.1	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 it states the management commitment and set out the organisational approach to managing information security.			
1.1.2	3.1.2	Review and evaluation	Whether the Security policy has an owner, who is responsible for its maintenance and review according to a defined review process. Whether the process ensures that a review takes place in response to any changes affecting the basis of the original assessment, example: significant security incidents, new vulnerabilities or changes to			

Information Security Management BS 7799.2:2002 Audit Check List						
Reference		Audit area, objective and question			Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance	
			organisational or technical infrastructure.			
Organisational Security						
2.1	4.1	<i>Information security infrastructure</i>				
2.1.1	4.1.1	Management information security forum	Whether there is a management forum to ensure there is a clear direction and visible management support for security initiatives within the organisation.			
2.1.2	4.1.2	Information security coordination	Whether there is a cross-functional forum of management representatives from relevant parts of the organisation to coordinate the implementation of information security controls.			
2.1.3	4.1.3	Allocation of information security responsibilities	Whether responsibilities for the protection of individual assets and for carrying out specific security processes were clearly defined.			
2.1.4	4.1.4	Authorisation process for information processing	Whether there is a management authorisation process in place for any new information processing facility. This should include all new facilities such as hardware and software.			

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
		facilities			
2.1.5	4.1.5	Specialist information security advise	Whether specialist information security advice is obtained where appropriate. A specific individual may be identified to co-ordinate in-house knowledge and experiences to ensure consistency, and provide help in security decision making.		
2.1.6	4.1.6	Co-operation between organisations	Whether appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunication operators were maintained to ensure that appropriate action can be quickly taken and advice obtained, in the event of a security incident.		
2.1.7	4.1.7	Independent review of information security	Whether the implementation of security policy is reviewed independently on regular basis. This is to provide assurance that organisational practices properly reflect the policy, and that it is feasible and effective.		
2.2	4.2	<i>Security of third party access</i>			
2.2.1	4.2.1	Identification of risks from third party	Whether risks from third party access are identified and appropriate security controls implemented. Whether the types of accesses are identified, classified		

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
		access	and reasons for access are justified.		
			Whether security risks with third party contractors working onsite was identified and appropriate controls are implemented.		
2.2.2	4.2.2	Security requirements in third party contracts	Whether there is a formal contract containing, or referring to, all the security requirements to ensure compliance with the organisation's security policies and standards.		
2.3	4.3	Outsourcing			
2.3.1	4.3.1	Security requirements in outsourcing contracts	<p>Whether security requirements are addressed in the contract with the third party, when the organisation has outsourced the management and control of all or some of its information systems, networks and/ or desktop environments.</p> <p>The contract should address how the legal requirements are to be met, how the security of the organisation's assets are maintained and tested, and the right of audit, physical security issues and how the availability of the services is to be maintained in the event of disaster.</p>		

Information Security Management BS 7799.2:2002 Audit Check List						
Reference		Audit area, objective and question			Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance	
Asset classification and control						
3.1	5.1	<i>Accountability of assets</i>				
3.1.1	5.1.1	Inventory of assets	Whether an inventory or register is maintained with the important assets associated with each information system. Whether each asset identified has an owner, the security classification defined and agreed and the location identified.			
3.2	5.2	<i>Information classification</i>				
3.2.1	5.2.1	Classification guidelines	Whether there is an Information classification scheme or guideline in place; which will assist in determining how the information is to be handled and protected.			
3.2.2	5.2.2	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 organisation.			
Personnel security						
4.1	6.1	<i>Security in job definition and Resourcing</i>				

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
4.1.1	6.1.1	Including security in job responsibilities	<p>Whether security roles and responsibilities as laid in Organisation's information security policy is documented where appropriate.</p> <p>This should include general responsibilities for implementing or maintaining security policy as well as specific responsibilities for protection of particular assets, or for extension of particular security processes or activities.</p>		
4.1.2	6.1.2	Personnel screening and policy	<p>Whether verification checks on permanent staff were carried out at the time of job applications.</p> <p>This should include character reference, confirmation of claimed academic and professional qualifications and independent identity checks.</p>		
4.1.3	6.1.3	Confidentiality agreements	<p>Whether employees are asked to sign Confidentiality or non-disclosure agreement as a part of their initial terms and conditions of the employment.</p> <p>Whether this agreement covers the security of the information processing facility and organisation assets.</p>		
4.1.4	6.1.4	Terms and conditions of employment	<p>Whether terms and conditions of the employment covers the employee's responsibility for information security. Where appropriate, these responsibilities might continue for a defined period after the end of the employment.</p>		

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
4.2	6.2	<i>User training</i>			
4.2.1	6.2.1	Information security education and training	Whether all employees of the organisation and third party users (where relevant) receive appropriate Information Security training and regular updates in organisational policies and procedures.		
4.3	6.3	<i>Responding to security incidents and malfunctions</i>			
4.3.1	6.3.1	Reporting security incidents	Whether a formal reporting procedure exists, to report security incidents through appropriate management channels as quickly as possible.		
4.3.2	6.3.2	Reporting security weaknesses	Whether a formal reporting procedure or guideline exists for users, to report security weakness in, or threats to, systems or services.		
4.3.3	6.3.3	Reporting software malfunctions	Whether procedures were established to report any software malfunctions.		
4.3.4	6.3.4	Learning from	Whether there are mechanisms in place to enable the types, volumes and costs of incidents and malfunctions		

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
		incidents	to be quantified and monitored.		
4.3.5	6.3.5	Disciplinary process	Whether there is a formal disciplinary process in place for employees who have violated organisational security policies and procedures. Such a process can act as a deterrent to employees who might otherwise be inclined to disregard security procedures.		
Physical and Environmental Security					
5.1	7.1	<i>Secure Area</i>			
5.1.1	7.1.1	Physical Security Perimeter	What physical border security facility has been implemented to protect the Information processing service. Some examples of such security facility are card control entry gate, walls, manned reception etc.,		
5.1.2	7.1.2	Physical entry Controls	What entry controls are in place to allow only authorised personnel into various areas within organisation.		
5.1.3	7.1.3	Securing Offices, rooms and facilities	Whether the rooms, which have the Information processing service, are locked or have lockable cabinets or safes.		

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
			Whether the Information processing service is protected from natural and man-made disaster.		
			Whether there is any potential threat from neighbouring premises.		
5.1.4	7.1.4	Working in Secure Areas	The information is only on need to know basis. Whether there exists any security control for third parties or for personnel working in secure area.		
5.1.5	7.1.5	Isolated delivery and loading areas	Whether the delivery area and information processing area are isolated from each other to avoid any unauthorised access.		
			Whether a risk assessment was conducted to determine the security in such areas.		
5.2	7.2	<i>Equipment Security</i>			
5.2.1	7.2.1	Equipment siting protection	Whether the equipment was located in appropriate place to minimise unnecessary access into work areas.		
			Whether the items requiring special protection were isolated to reduce the general level of protection required.		

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
			Whether controls were adopted to minimise risk from potential threats such as theft, fire, explosives, smoke, water, dist, vibration, chemical effects, electrical supply interfaces, electromagnetic radiation, flood.		
			Whether there is a policy towards eating, drinking and smoking on in proximity to information processing services.		
			Whether environmental conditions are monitored which would adversely affect the information processing facilities.		
5.2.2	7.2.2	Power Supplies	Whether the equipment is protected from power failures by using permanence of power supplies such as multiple feeds, uninterruptible power supply (ups), backup generator etc.,		
5.2.3	7.2.3	Cabling Security	Whether the power and telecommunications cable carrying data or supporting information services are protected from interception or damage.		
			Whether there are any additional security controls in place for sensitive or critical information.		
5.2.4	7.2.4	Equipment Maintenance	Whether the equipment is maintained as per the supplier's recommended service intervals and specifications. Whether the maintenance is carried out only by authorised personnel.		

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
			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. If the equipment is covered by insurance, whether the insurance requirements are satisfied.		
5.2.5	7.2.5	Securing of equipment off-premises	Whether any equipment usage outside an organisation's premises for information processing has to be authorised by the management.		
			Whether the security provided for these equipments while outside the premises are on par with or more than the security provided inside the premises.		
5.2.6	7.2.6	Secure disposal or re-use of equipment	Whether storage device containing sensitive information are physically destroyed or securely over written.		
5.3	7.3	<i>General Controls</i>			
5.3.1	7.3.1	Clear Desk and clear screen	Whether automatic computer screen locking facility is enabled. This would lock the screen when the computer is left unattended for a period.		

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
		policy	Whether employees are advised to leave any confidential material in the form of paper documents, media etc., in a locked manner while unattended.		
5.3.2	7.3.2	Removal of property	Whether equipment, information or software can be taken offsite without appropriate authorisation.		
			Whether spot checks or regular audits were conducted to detect unauthorised removal of property. Whether individuals are aware of these types of spot checks or regular audits.		
Communications and Operations Management					
6.1	8.1	<i>Operational Procedure and responsibilities</i>			
6.1.1	8.1.1	Documented Operating procedures	Whether the Security Policy has identified any Operating procedures such as Back-up, Equipment maintenance etc.,		
			Whether such procedures are documented and used.		
6.1.2	8.1.2	Operational Change	Whether all programs running on production systems are subject to strict change control i.e., any change to be made to those production programs need to go		

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
		Control	through the change control authorisation.		
			Whether audit logs are maintained for any change made to the production programs.		
6.1.3	8.1.3	Incident management procedures	Whether an Incident Management procedure exist to handle security incidents.		
			Whether the procedure addresses the incident management responsibilities, orderly and quick response to security incidents.		
			Whether the procedure addresses different types of incidents ranging from denial of service to breach of confidentiality etc., and ways to handle them.		
			Whether the audit trails and logs relating to the incidents are maintained and proactive action taken in a way that the incident doesn't reoccur.		
6.1.4	8.1.4	Segregation of duties	Whether duties and areas of responsibility are separated in order to reduce opportunities for unauthorised modification or misuse of information or services.		
6.1.5	8.1.5	Separation of development	Whether the development and testing facilities are isolated from operational facilities. For example development software should run on a different computer to that of the computer with production		

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
		and operational facilities	software. Where necessary development and production network should be separated from each other.		
6.1.6	8.1.6	External facilities management	Whether any of the Information processing facility is managed by external company or contractor (third party).		
			Whether the risks associated with such management is identified in advance, discussed with the third party and appropriate controls were incorporated into the contract. Whether necessary approval is obtained from business and application owners.		
6.2	8.2	<i>System planning and acceptance</i>			
6.2.1	8.2.1	Capacity Planning	Whether the capacity demands are monitored and projections of future capacity requirements are made. This is to ensure that adequate processing power and storage are available. Example: Monitoring Hard disk space, RAM, CPU on critical servers.		
6.2.2	8.2.2	System	Whether System acceptance criteria are established for new information systems, upgrades and new versions.		

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
		acceptance	Whether suitable tests were carried out prior to acceptance.		
6.3	8.3	<i>Protection against malicious software</i>			
6.3.1	8.3.1	Control against malicious software	Whether there exists any control against malicious software usage.		
			Whether the security policy does address software licensing issues such as prohibiting usage of unauthorised software.		
			Whether there exists any Procedure to verify all warning bulletins are accurate and informative with regards to the malicious software usage.		
			Whether Antivirus software is installed on the computers to check and isolate or remove any viruses from computer and media. Whether this software signature is updated on a regular basis to check any latest viruses.		
			Whether all the traffic originating from un-trusted network in to the organisation is checked for viruses. Example: Checking for viruses on email, email attachments and on the web, FTP traffic.		
6.4	8.4	<i>Housekeeping</i>			

Information Security Management BS 7799.2:2002 Audit Check List						
Reference		Audit area, objective and question		Results		
Checklist	Standard	Section	Audit Question	Findings	Compliance	
6.4.1	8.4.1	Information back-up	Whether Back-up of essential business information such as production server, critical network components, configuration backup etc., were taken regularly. Example: Mon-Thu: Incremental Backup and Fri: Full Backup.			
			Whether the backup media along with the procedure to restore the backup are stored securely and well away from the actual site.			
			Whether the backup media are regularly tested to ensure that they could be restored within the time frame allotted in the operational procedure for recovery.			
6.4.2	8.4.2	Operator logs	Whether Operational staffs maintain a log of their activities such as name of the person, errors, corrective action etc., Whether Operator logs are checked on regular basis against the Operating procedures.			
6.4.3	8.4.3		Fault Logging	Whether faults are reported and well managed. This includes corrective action being taken, review of the fault logs and checking the actions taken		
6.5	8.5	<i>Network Management</i>				

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
6.5.1	8.5.1	Network Controls	Whether effective operational controls such as separate network and system administration facilities were be established where necessary.		
			Whether responsibilities and procedures for management of remote equipment, including equipment in user areas were established.		
			Whether there exist any special controls to safeguard confidentiality and integrity of data processing over the public network and to protect the connected systems. Example: Virtual Private Networks, other encryption and hashing mechanisms etc.,		
6.6	8.6	<i>Media handling and Security</i>			
6.6.1	8.6.1	Management of removable computer media	Whether there exist a procedure for management of removable computer media such as tapes, disks, cassettes, memory cards and reports.		
6.6.2	8.6.2	Disposal of Media	Whether the media that are no longer required are disposed off securely and safely.		
			Whether disposal of sensitive items are logged where necessary in order to maintain an audit trail.		

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
6.6.3	8.6.3	Information handling procedures	Whether there exists a procedure for handling the storage of information. Does this procedure address issues such as information protection from unauthorised disclosure or misuse.		
6.6.4	8.6.4	Security of system documentation	Whether the system documentation is protected from unauthorised access. Whether the access list for the system documentation is kept to minimum and authorised by the application owner. Example: System documentation need to be kept on a shared drive for specific purposes, the document need to have Access Control Lists enabled (to be accessible only by limited users.)		
6.7	8.7	<i>Exchange of Information and software</i>			
6.7.1	8.7.1	Information and software exchange agreement	Whether there exists any formal or informal agreement between the organisations for exchange of information and software.		
			Whether the agreement does addresses the security issues based on the sensitivity of the business information involved.		

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
6.7.2	8.7.2	Security of Media in transit	Whether security of media while being transported taken into account.		
			Whether the media is well protected from unauthorised access, misuse or corruption.		
6.7.3	8.7.3	Electronic Commerce security	Whether Electronic commerce is well protected and controls implemented to protect against fraudulent activity, contract dispute and disclosure or modification of information.		
			Whether Security controls such as Authentication, Authorisation are considered in the ECommerce environment.		
			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.		
6.7.4	8.7.4	Security of Electronic email	Whether there is a policy in place for the acceptable use of electronic mail or does security policy does address the issues with regards to use of electronic mail.		
			Whether controls such as antivirus checking, isolating potentially unsafe attachments, spam control, anti relaying etc., are put in place to reduce the risks created by electronic email.		

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
6.7.5	8.7.5	Security of Electronic office systems	Whether there is an Acceptable use policy to address the use of Electronic office systems.		
			Whether there are any guidelines in place to effectively control the business and security risks associated with the electronic office systems.		
6.7.6	8.7.6	Publicly available systems	Whether there is any formal authorisation process in place for the information to be made publicly available. Such as approval from Change Control which includes Business, Application owner etc.,		
			Whether there are any controls in place to protect the integrity of such information publicly available from any unauthorised access. This might include controls such as firewalls, Operating system hardening, any Intrusion detection type of tools used to monitor the system etc.,		
6.7.7	8.7.7	Other forms of information exchange	Whether there are any policies, procedures or controls in place to protect the exchange of information through the use of voice, facsimile and video communication facilities.		
			Whether staffs are reminded to maintain the confidentiality of sensitive information while using such forms of information exchange facility.		

Information Security Management BS 7799.2:2002 Audit Check List						
Reference		Audit area, objective and question			Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance	
Access Control						
7.1	9.1	<i>Business Requirements for Access Control</i>				
7.1.1	9.1.1	Access Control Policy	Whether the business requirements for access control have been defined and documented.			
			Whether the Access control policy does address the rules and rights for each user or a group of user.			
			Whether the users and service providers were given a clear statement of the business requirement to be met by access controls.			
7.2	9.2	<i>User Access Management</i>				
7.2.1	9.2.1	User Registration	Whether there is any formal user registration and de-registration procedure for granting access to multi-user information systems and services.			
7.2.2	9.2.2	Privilege Management	Whether the allocation and use of any privileges in multi-user information system environment is restricted and controlled i.e., Privileges are allocated on need-to-use basis; privileges are allocated only after formal authorisation process.			

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
7.2.3	9.2.3	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.		
7.2.4	9.2.4	Review of user access rights	Whether there exist a process to review user access rights at regular intervals. Example: Special privilege review every 3 months, normal privileges every 6 moths.		
7.3	9.3	<i>User Responsibilities</i>			
7.3.1	9.3.1	Password use	Whether there are any guidelines in place to guide users in selecting and maintaining secure passwords.		
7.3.2	9.3.2	Unattended user equipment	Whether the users and contractors are made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibility to implement such protection. Example: Logoff when session is finished or set up auto log off, terminate sessions when finished etc.,		
7.4	9.4	<i>Network Access Control</i>			
7.4.1	9.4.1	Policy on use of	Whether there exists a policy that does address concerns relating to networks and network services		

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
		network services	such as: Parts of network to be accessed, Authorisation services to determine who is allowed to do what, Procedures to protect the access to network connections and network services.		
7.4.2	9.4.2	Enforced path	Whether there is any control that restricts the route between the user terminal and the designated computer services the user is authorised to access example: enforced path to reduce the risk.		
7.4.3	9.4.3	User authentication for external connections	Whether there exist any authentication mechanism for challenging external connections. Examples: Cryptography based technique, hardware tokens, software tokens, challenge/ response protocol etc.,		
7.4.4	9.4.4	Node Authentication	Whether connections to remote computer systems that are outside organisations security management are authenticated. Node authentication can serve as an alternate means of authenticating groups of remote users where they are connected to a secure, shared computer facility.		
7.4.5	9.4.5	Remote diagnostic port	Whether accesses to diagnostic ports are securely controlled i.e., protected by a security mechanism.		

Information Security Management BS 7799.2:2002 Audit Check List						
Reference		Audit area, objective and question		Results		
Checklist	Standard	Section	Audit Question	Findings	Compliance	
		protection				
7.4.6	9.4.6	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.			
7.4.7	9.4.7	Network connection protocols	Whether there exists any network connection control for shared networks that extend beyond the organisational boundaries. Example: electronic mail, web access, file transfers, etc.,			
7.4.8	9.4.8	Network routing control	Whether there exist any network control to ensure that computer connections and information flows do not breach the access control policy of the business applications. This is often essential for networks shared with non-organisations users.			
			Whether the routing controls are based on the positive source and destination identification mechanism. Example: Network Address Translation (NAT).			
7.4.9	9.4.9	Security of network services	Whether the organisation, using public or private network service does ensure that a clear description of security attributes of all services used is provided.			
7.5	9.5	<i>Operating system access control</i>				

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
7.5.1	9.5.1	Automatic terminal identification	Whether automatic terminal identification mechanism is used to authenticate connections.		
7.5.2	9.5.2	Terminal log-on procedures	Whether access to information system is attainable only via a secure log-on process.		
			Whether there is a procedure in place for logging in to an information system. This is to minimise the opportunity of unauthorised access.		
7.5.3	9.5.3	User identification and authorisation	Whether unique identifier is provided to every user such as operators, system administrators and all other staff including technical. The generic user accounts should only be supplied under exceptional circumstances where there is a clear business benefit. Additional controls may be necessary to maintain accountability.		
			Whether the authentication method used does substantiate the claimed identity of the user; commonly used method: Password that only the user knows.		
7.5.4	9.5.4	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,		

Information Security Management BS 7799.2:2002 Audit Check List						
Reference		Audit area, objective and question		Results		
Checklist	Standard	Section	Audit Question	Findings	Compliance	
			not display passwords on screen etc.,			
7.5.5	9.5.5	Use of system utilities	Whether the system utilities that comes with computer installations, but may override system and application control is tightly controlled.			
7.5.6	9.5.6	Duress alarm to safeguard users	Whether provision of a duress alarm is considered for users who might be the target of coercion.			
7.5.7	9.5.7	Terminal time-out	Inactive terminal in public areas should be configured to clear the screen or shut down automatically after a defined period of inactivity.			
7.5.8	9.5.8	Limitation of connection time	Whether there exist any 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	9.6	<i>Application Access Control</i>				
7.6.1	9.6.1	Information access restriction	Whether access to application by various groups/ personnel within the organisation should be defined in the access control policy as per the individual business application requirement and is consistent with the organisation's Information access policy.			

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
7.6.2	9.6.2	Sensitive system isolation	Whether sensitive systems are provided with isolated computing environment such as running on a dedicated computer, share resources only with trusted application systems, etc.,		
7.7	9.7	<i>Monitoring system access and use</i>			
7.7.1	9.7.1	Event logging	Whether audit logs recording exceptions and other security relevant events are produced and kept for an agreed period to assist in future investigations and access control monitoring.		
7.7.2	9.7.2	Monitoring system use	Whether procedures are set up for monitoring the use of information processing facility. The procedure should ensure that the users are performing only the activities that are explicitly authorised.		
			Whether the results of the monitoring activities are reviewed regularly.		
7.7.3	9.7.3	Clock synchronisation	Whether the computer or communication device has the capability of operating a real time clock, it should be set to an agreed standard such as Universal co-ordinated time or local standard time. The correct setting of the computer clock is important to ensure the accuracy of the audit logs.		

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
7.8	9.8	Mobile computing and teleworking			
7.8.1	9.8.1	Mobile computing	Whether a formal policy is adopted that takes into account the risks of working with computing facilities such as notebooks, palmtops etc., especially in unprotected environments.		
			Whether trainings were arranged for staff to use mobile computing facilities to raise their awareness on the additional risks resulting from this way of working and controls that need to be implemented to mitigate the risks.		
7.8.2	9.8.2	Teleworking	Whether there is any policy, procedure and/ or standard to control teleworking activities, this should be consistent with organisation's security policy.		
			Whether suitable protection of teleworking site is in place against threats such as theft of equipment, unauthorised disclosure of information etc.,		
System development and maintenance					
8.1	10.1	Security requirements of systems			
8.1.1	10.1.1	Security requirements	Whether security requirements are incorporated as part of business requirement statement for new systems or for enhancement to existing systems.		

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
		analysis and specification	Security requirements and controls identified should reflect business value of information assets involved and the consequence from failure of Security.		
			Whether risk assessments are completed prior to commencement of system development.		
8.2	10.2	<i>Security in application systems</i>			
8.2.1	10.2.1	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 type 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	10.2.2	Control of internal processing	Whether areas of risks are identified in the processing cycle and validation checks were included. In some cases the data that has been correctly entered can be corrupted by processing errors or through deliberate acts.		
			Whether appropriate controls are identified for applications to mitigate from risks during internal processing. The controls will depend on nature of application and business impact of any corruption of data.		

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
8.2.3	10.2.3	Message authentication	<p>Whether an assessment of security risk was carried out to determine if Message authentication is required; and to identify most appropriate method of implementation if it is necessary.</p> <p>Message authentication is a technique used to detect unauthorised changes to, or corruption of, the contents of the transmitted electronic message.</p>		
8.2.4	10.2.4	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	10.3	<i>Cryptographic controls</i>			
8.3.1	10.3.1	Policy on use of cryptographic controls	<p>Whether there is a “Policy in use of cryptographic controls for protection of information” is in place.</p> <p>Whether a risk assessment was carried out to identify the level of protection the information should be given.</p>		
8.3.2	10.3.2	Encryption	<p>Whether encryption techniques were used to protect the data.</p> <p>Whether assessments were conducted to analyse the sensitivity of the data and the level of protection needed.</p>		
8.3.3	10.3.3	Digital	Whether Digital signatures were used to protect the		

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
		Signatures	authenticity and integrity of electronic documents.		
8.3.4	10.3.4	Non-repudiation services	Whether non-repudiation services were used, where it might be necessary to resolve disputes about occurrence or non-occurrence of an event or action. Example: Dispute involving use of a digital signature on an electronic payment or contract.		
8.3.5	10.3.5	Key management	Whether there is a management system is in place to support the organisation's use of cryptographic techniques such as Secret key technique and Public key technique.		
			Whether the Key management system is based on agreed set of standards, procedures and secure methods.		
8.4	10.4	<i>Security of system files</i>			
8.4.1	10.4.1	Control of operational software	Whether there are any controls in place for the implementation of software on operational systems. This is to minimise the risk of corruption of operational systems.		
8.4.2	10.4.2	Protection of system test data	Whether system test data is protected and controlled. The use of operational database containing personal information should be avoided for test purposes. If such information is used, the data should be depersonalised before use.		

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
8.4.3	10.4.3	Access Control to program source library	Whether strict controls are in place over access to program source libraries. This is to reduce the potential for corruption of computer programs.		
8.5	10.5	<i>Security in development and support process</i>			
8.5.1	10.5.1	Change control procedures	Whether there are strict control procedures in place over implementation of changes to the information system. This is to minimise the corruption of information system.		
8.5.2	10.5.2	Technical review of operating system changes	Whether there are process or procedure in place to ensure application system is reviewed and tested after change in operating system. Periodically it is necessary to upgrade operating system i.e., to install service packs, patches, hot fixes etc.,		
8.5.3	10.5.3	Technical review of operating system changes	Whether there are any restrictions in place to limit changes to software packages. As far as possible the vendor supplied software packages should be used without modification. If changes are deemed essential the original software should be retained and the changes applied only to a clearly identified copy. All changes should be clearly tested and documented, so they can be reapplied if necessary to future software upgrades.		

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
8.5.4	10.5.4	Covert channels and Trojan code	<p>Whether there are controls in place to ensure that the covert channels and Trojan codes are not introduced into new or upgraded system.</p> <p>A covert channel can expose information by some indirect and obscure means. Trojan code is designed to affect a system in a way that is not authorised.</p>		
8.5.5	10.5.5	Outsourced software development	<p>Whether there are controls in place over outsourcing software.</p> <p>The points to be noted includes: Licensing arrangements, escrow arrangements, contractual requirement for quality assurance, testing before installation to detect Trojan code etc.,</p>		
Business Continuity Management					
9.1	11.1	<i>Aspects of Business Continuity Management</i>			
9.1.1	11.1.1	Business continuity management process	<p>Whether there is a managed process in place for developing and maintaining business continuity throughout the organisation.</p> <p>This might include Organisation wide Business continuity plan, regular testing and updating of the plan, formulating and documenting a business continuity strategy etc.,</p>		

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
9.1.2	11.1.2	Business continuity and impact analysis	<p>Whether events that could cause interruptions to business process were identified example: equipment failure, flood and fire.</p> <p>Whether a risk assessment was conducted to determine impact of such interruptions.</p> <p>Whether a strategy plan was developed based on the risk assessment results to determine an overall approach to business continuity.</p>		
9.1.3	11.1.3	Writing and implementing continuity plan	<p>Whether plans were developed to restore business operations within the required time frame following an interruption or failure to business process.</p> <p>Whether the plan is regularly tested and updated.</p>		
9.1.4	11.1.4	Business continuity planning framework	<p>Whether there is a single framework of Business continuity plan.</p> <p>Whether this framework is maintained to ensure that all plans are consistent and identify priorities for testing and maintenance.</p> <p>Whether this identifies conditions for activation and individuals responsible for executing each component of the plan.</p>		
9.1.5	11.1.5	Testing, maintaining and re-	<p>Whether Business continuity plans are tested regularly to ensure that they are up to date and effective.</p>		

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
		assessing business continuity plan			
			<p>Whether Business continuity plans were maintained by regular reviews and updates to ensure their continuing effectiveness.</p> <p>Whether procedures were included within the organisations change management programme to ensure that Business continuity matters are appropriately addressed.</p>		
Compliance					
10.1	12.1	<i>Compliance with legal requirements</i>			
10.1.1	12.1.1	Identification of applicable legislation	<p>Whether all relevant statutory, regulatory and contractual requirements were explicitly defined and documented for each information system.</p> <p>Whether specific controls and individual responsibilities to meet these requirements were defined and documented.</p>		
10.1.2	12.1.2	Intellectual property rights	Whether there exist any procedures to ensure compliance with legal restrictions on use of material in respect of which there may be intellectual property		

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
		(IPR)	rights such as copyright, design rights, trade marks. Whether the procedures are well implemented.		
			Whether proprietary software products are supplied under a license agreement that limits the use of the products to specified machines. The only exception might be for making own back-up copies of the software.		
10.1.3	12.1.3	Safeguarding of organisational records	Whether important records of the organisation is protected from loss destruction and falsi function.		
10.1.4	12.1.4	Data protection and privacy of personal information	Whether there is a management structure and control in place to protect data and privacy of personal information.		
10.1.5	12.1.5	Prevention of misuse of information processing	Whether use of information processing facilities for any non-business or unauthorised purpose, without management approval is treated as improper use of the facility. Whether at the log-on a warning message is presented on the computer screen indicating that the system		

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
		facility	being entered is private and that unauthorised access is not permitted.		
10.1.6	12.1.6	Regulation of cryptographic controls	Whether the regulation of cryptographic control is as per the sector and national agreement.		
10.1.7	12.1.7	Collection of evidence	Whether the process involved in collecting the evidence is in accordance with legal and industry best practise.		
10.2	12.2	<i>Reviews of Security Policy and technical compliance</i>			
10.2.1	12.2.1	Compliance with security policy	Whether all areas within the organisation is considered for regular review to ensure compliance with security policy, standards and procedures.		
10.2.2	12.2.2	Technical compliance checking	Whether information systems were regularly checked for compliance with security implementation standards. Whether the technical compliance check is carried out by, or under the supervision of, competent, authorised persons.		
10.3	12.3	<i>System audit considerations</i>			

Information Security Management BS 7799.2:2002 Audit Check List					
Reference		Audit area, objective and question		Results	
Checklist	Standard	Section	Audit Question	Findings	Compliance
10.3.1	12.3.1	System audit controls	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.		
10.3.2	12.3.2	Protection of system audit tools	Whether access to system audit tools such as software or data files are protected to prevent any possible misuse or compromise.		

References

1. Information Security Management, Part2: Specification for Information security management systems AS/NZS 7799.2:2003
BS 7799.2:2002
2. Information Technology – Code of practice for Information Security Management AS/NZS ISO/IEC 17799:2001



Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

SANS Essentials Australia 2021	OnlineAU	Feb 15, 2021 - Feb 20, 2021	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced