Nr.	Controls in ISO/IEC 27001:2005 Annex A	Organizational control	Technical control	System testing (Console) possible recommended required	Visual inspection	Audit review guidance
A.5	Security Policy					
A.5.1	Information Security Policy					
A.5.1.1	Information security policy document	X				
A.5.1.2	Review of the information security policy	X				management review minutes
A.6	Organization of information security					
A.6.1	Internal organization					
A.6.1.1	Management commitment to information security	X				management meeting minutes
A.6.1.2	Information security co-ordination	X				management meeting minutes
A.6.1.3	Allocation of information security responsibilities	X				
A.6.1.4	Authorization process for information processing facilities	X				check the inventory
A.6.1.5	Confidentiality agreements	X				sample some copies from files
A.6.1.6	Contact with authorities	X				
A.6.1.7	Contact with special interest groups	X				
A.6.1.8	Independent review of information security	X				read the reports
A.6.2	External parties					
A.6.2.1	Identification of risks related to external parties	X				
A.6.2.2	Addressing security when dealing with customers	X				
A.6.2.3	Addressing security in third party agreements	X				test some contract conditions
A.7	Asset management					
A.7.1	Responsibility for assets					
A.7.1.1	Inventory of assets	X				identify the assets
A.7.1.2	Ownership of assets	X				
A.7.1.3	Acceptable use of assets	X				

Nr.	Controls in ISO/IEC 27001:2005 Annex A	Organizational control	Technical control	System testing (Console) possible recommended required	Visual inspection	Audit review guidance
A.7.2	Information classification					
A.7.2.1	Classification guidelines	X				
A.7.2.2	Information labeling and handling	X				naming: Directories, files, printed reports, recorded media (e.g. tapes, disks, CDs), electronic messages and file transfers.
A.8	Human resources security					
A.8.1	Prior to employment					
A.8.1.1	Roles and responsibilities	X				
A.8.1.2	Screening	X				
A.8.1.3	Terms and conditions of employment	X				
A.8.2	During employment					
A.8.2.1	Management responsibilities	X				
A.8.2.2	Information security awareness, education and training	X				ask staff if they are aware of specific things they should be aware of
A.8.2.3	Disciplinary process	X				
A.8.3	Termination or change of employment					
A.8.3.1	Termination responsibilities	X				
A.8.3.2	Return of assets	X				
A.8.3.3	Removal of access rights	X	X	recommended		
A.9	Physical and environmental security					
A.9.1	Secure areas					
A.9.1.1	Physical security perimeter	X				
A.9.1.2	Physical entry controls	X	X	possible	X	archiving of access records
A.9.1.3	Securing offices, rooms and facilities	X			X	
A.9.1.4	Protecting against external and environmental threats	X			X	
A.9.1.5	Working in secure areas	X			X	
A.9.1.6	Public access, delivery and loading areas	X			X	

Nr.	Controls in ISO/IEC 27001:2005 Annex A	Organizational control	Technical control	System testing (Console) possible recommended required	Visual inspection	Audit review guidance
A.9.2	Equipment security					
A.9.2.1	Equipment siting and protection	X		possible	X	
A.9.2.2	Supporting utilities	X	X	possible	X	
A.9.2.3	Cabling security	X			X	
A.9.2.4	Equipment maintenance	X				
A.9.2.5	Security of equipment off premises	X	X	possible		portable device encryption
A.9.2.6	Secure disposal or re-use of equipment	X	X	possible	X	
A.9.2.7	Removal of property	X				
A.10	Communications and operations management					
A.10.1	Operational procedures and responsibilities					
A.10.1.1	Documented operating procedures	X				
A.10.1.2	Change management	X	X	recommended		
A.10.1.3	Segregation of duties	X				
A.10.1.4	Separation of development, test and operational facilities	X	X	possible		
A.10.2	Third party service delivery management					
A.10.2.1	Service delivery	X				
A.10.2.2	Monitoring and review of third party services	X	X	possible		
A.10.2.3	Managing changes to third party services	X				
A.10.3	System planning and acceptance					
A.10.3.1	Capacity management	X	X	possible		
A.10.3.2	System acceptance	X				
A.10.4	Protection against malicious and mobile code					
A.10.4.1	Controls against malicious code	X	X	required		sample of servers, desktops, gateways
A.10.4.2	Controls against mobile code	X	X	possible		active content
A.10.5	Back -up					
A.10.5.1	Information back-up	X	X	recommended		try a recovery

Nr.	Controls in ISO/IEC 27001:2005 Annex A	Organizational control	Technical control	System testing (Console) possible recommended required	Visual inspection	Audit review guidance
A.10.6	Network security management					
A.10.6.1	Network controls	X	X	possible		
A.10.6.2	Security of network services	X				SLA's, security features
A.10.7	Media handling					
A.10.7.1	Management of removable media	X	X	possible		
A.10.7.2	Disposal of media	X				
A.10.7.3	Information handling procedures	X				
A.10.7.4	Security of system documentation	X	X	possible	X	
A.10.8	Exchange of information					
A.10.8.1	Information exchange policies and procedures	X				
A.10.8.2	Exchange agreements	X				
A.10.8.3	Physical media in transit	X	X	possible		encryption or physical protection
A.10.8.4	Electronic messaging	X	X	possible		confirm sample messages conform to policy/procedures
A.10.8.5	Business information systems	X				
A.10.9	Electronic commerce services					
A.10.9.1	Electronic commerce	X	X	possible		
A.10.9.2	On-line transactions	X	X	recommended		check: integrity, access authorization
A.10.9.3	Publicly available information	X	X	possible		
A.10.10	Monitoring					
A.10.10.1	Audit logging	X	X	possible		on-line or printed
A.10.10.2	Monitoring system use	X	X	possible		
A.10.10.3	Protection of log information	X	X	possible		
A.10.10.4	Administrator and operator logs	X	X	possible		
A.10.10.5	Fault logging	X				
A.10.10.6	Clock synchronization		X	possible		time restricted authentication methods

Nr.	Controls in ISO/IEC 27001:2005 Annex A	Organizational control	Technical control	System testing (Console) possible recommended required	Visual inspection	Audit review guidance
A.11	Access control					
A.11.1	Business requirement for access control					
A.11.1.1	Access control policy	X				
A.11.2	User access management					
A.11.2.1	User registration	X				sample employees/contractors to authorizations for all access rights to all systems
A.11.2.2	Privilege management	X	X	possible		internal transfer of staff
A.11.2.3	User password management	X				
A.11.2.4	Review of user access rights	X				
A.11.3	User responsibilities					
A.11.3.1	Password use	X				verify guidelines/policy in place for users
A.11.3.2	Unattended user equipment	X				verify guidelines/policy in place for users
A.11.3.3	Clear desk and clear screen policy	X			X	
A.11.4	Network access control					
A.11.4.1	Policy on use of network services	X				
A.11.4.2	User authentication for external connections	X	X	required		
A.11.4.3	Equipment identification in networks		X			
A.11.4.4	Remote diagnostic and configuration port protection		X	recommended		
A.11.4.5	Segregation in networks	X	X	possible		network diagrams: WAN, LAN, VLAN, VPN, network objects, network segments (e.g. DMZ)
A.11.4.6	Network connection control	X	X	recommended		shared networks not very common
A.11.4.7	Network routing control	X	X	required		Firewalls, Routers/Switches: Rulebase, ACL's, Routing, Access Control Policies
A.11.5	Operating system access control					
A.11.5.1	Secure log-on procedures	X	X	recommended		
A.11.5.2	User identification and authentication	X	X	recommended		
A.11.5.3	Password management system	X	X	recommended		
A.11.5.4	Use of system utilities	X	X	recommended		

Nr.	Controls in ISO/IEC 27001:2005 Annex A	Organizational control	Technical control	System testing (Console) possible recommended required	Visual inspection	Audit review guidance
A.11.5.5	Session time-out	X	X	possible	X	
A.11.5.6	Limitation of connection time	X	X	possible	X	
A.11.6	Application and information access control					
A.11.6.1	Information access restriction	X	X	required		system settings and configurations
A.11.6.2	Sensitive system isolation	X	X	possible		
A.11.7	Mobile computing and teleworking					
A.11.7.1	Mobile computing and communications	X	X	possible		
A.11.7.2	Teleworking	X	X	possible		
A.12	Information systems acquisition, development and maintenance					
A.12.1	Security requirements of information systems					
A.12.1.1	Security requirements analysis and specification	X				
A.12.2	Correct processing in applications					
A.12.2.1	Input data validation	X	X	recommended		software development guidelines, SW testing; confirm in sample business applications that controls required by the users exist in practice
A.12.2.2	Control of internal processing	X	X	possible		software development guidelines, SW testing; confirm in sample business applications that controls required by the users exist in practice
A.12.2.3	Message integrity		X	possible		
A.12.2.4	Output data validation	X	X	possible		software development guidelines, SW testing; confirm in sample business applications that controls required by the users exist in practice
A.12.3	Cryptographic controls					
A.12.3.1	Policy on the use of cryptographic controls	X	X	possible		also check implementation of policy where appropriate
A.12.3.2	Key management	X	X	required		
A.12.4	Security of system files					
A.12.4.1	Control of operational software	X	X	possible		

Nr.	Controls in ISO/IEC 27001:2005 Annex A	Organizational control	Technical control	System testing (Console) possible recommended required	Visual inspection	Audit review guidance
A.12.4.2	Protection of system test data	X	X	possible	X	
A.12.4.3	Access control to program source code	X	X	recommended		
A.12.5	Security in development and support processes					
A.12.5.1	Change control procedures	X				
A.12.5.2	Technical review of applications after operating system changes	X				
A.12.5.3	Restrictions on changes to software packages	X				
A.12.5.4	Information leakage	X	X	possible		unknown services
A.12.5.5	Outsourced software development	X				
A.12.6	Technical Vulnerability Management					
A.12.6.1	Control of technical vulnerabilities	X	X	required		patch distribution
A.13	Information security incident management					
A.13.1	Reporting information security events and weaknesses					
A.13.1.1	Reporting information security events	X				
A.13.1.2	Reporting security weaknesses	X				
A.13.2	Management of information security incidents and improvements					
A.13.2.1	Responsibilities and procedures	X				
A.13.2.2	Learning from information security incidents	X				
A.13.2.3	Collection of evidence	X				
A.14	Business continuity management					
A.14.1	Information security aspects of business continuity management					
A.14.1.1	Including information security in the business continuity management process	X				
A.14.1.2	Business continuity and risk assessment	X				

Nr.	Controls in ISO/IEC 27001:2005 Annex A	Organizational control	Technical control	System testing (Console) possible recommended required	Visual inspection	Audit review guidance
A.14.1.3	Developing and implementing continuity plans including information security	X	X	possible	X	DR-Site inspection, distance of DR-site according to risk assessment and applicable legal/regulatory requirements
A.14.1.4	Business continuity planning framework	X				
A.14.1.5	Testing maintaining and reassessing business continuity plans	X				
A.15	Compliance					
A.15.1	Compliance with legal requirements					
A.15.1.1	Identification of applicable legislation	X				
A.15.1.2	Intellectual property rights (IPR)	X				
A.15.1.3	Protection of organizational records	X	X	possible		
A.15.1.4	Data protection and privacy of personal information	X	X	possible		
A.15.1.5	Prevention of misuse of information processing facilities	X				
A.15.1.6	Regulation of cryptographic controls	X				
A.15.2	Compliance with security policies and standards, and technical compliance					
A.15.2.1	Compliance with security policies and standards	X				
A.15.2.2	Technical compliance checking	X	X			assess process and follow-up
A.15.3	Information systems audit considerations					
A.15.3.1	Information systems audit controls	X				
A.15.3.2	Protection of information systems audit tools	X	X	possible		