Enterprise Standards and Best Practices for IT Infrastructure

Lab Report

Lab 04 - ISO27001_SOA_DOCUMENT

IT 120 62 966 – S.H.U.S.Wickramarathne

WEEKEND IT

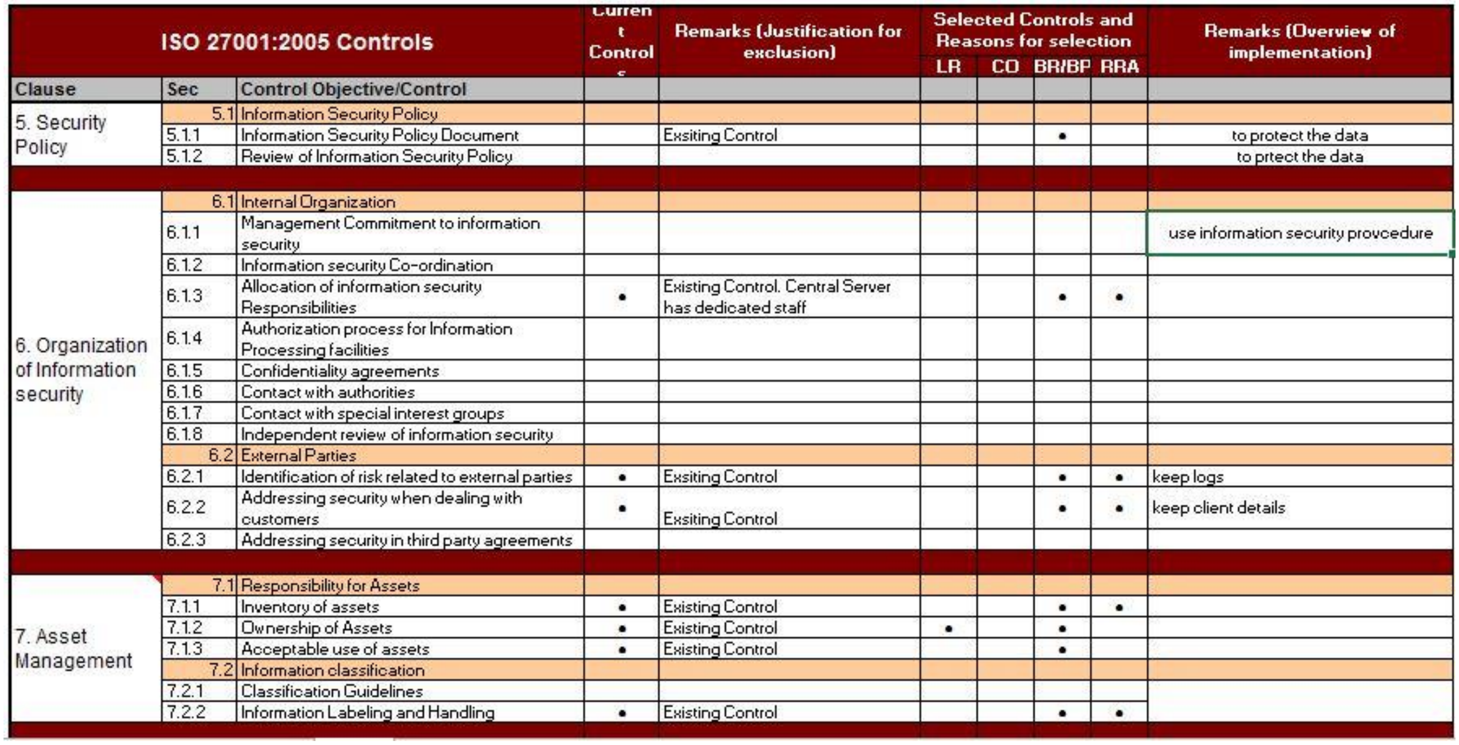
COMPUTING | BUSINESS | ENGINEERING

Sri Lanka Institute of Information Technology

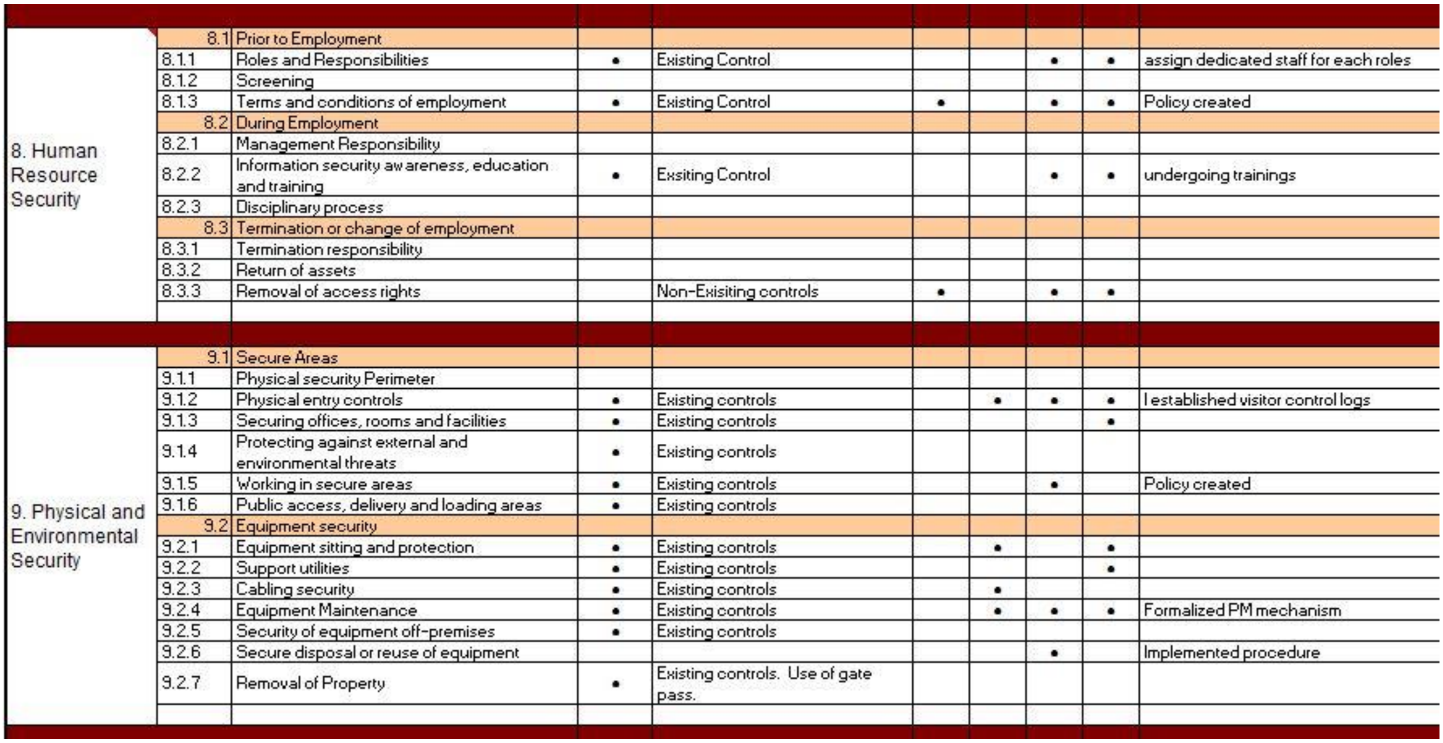
B.Sc. Special (Honors) Degree in Information Technology

Specialized in Information Technology

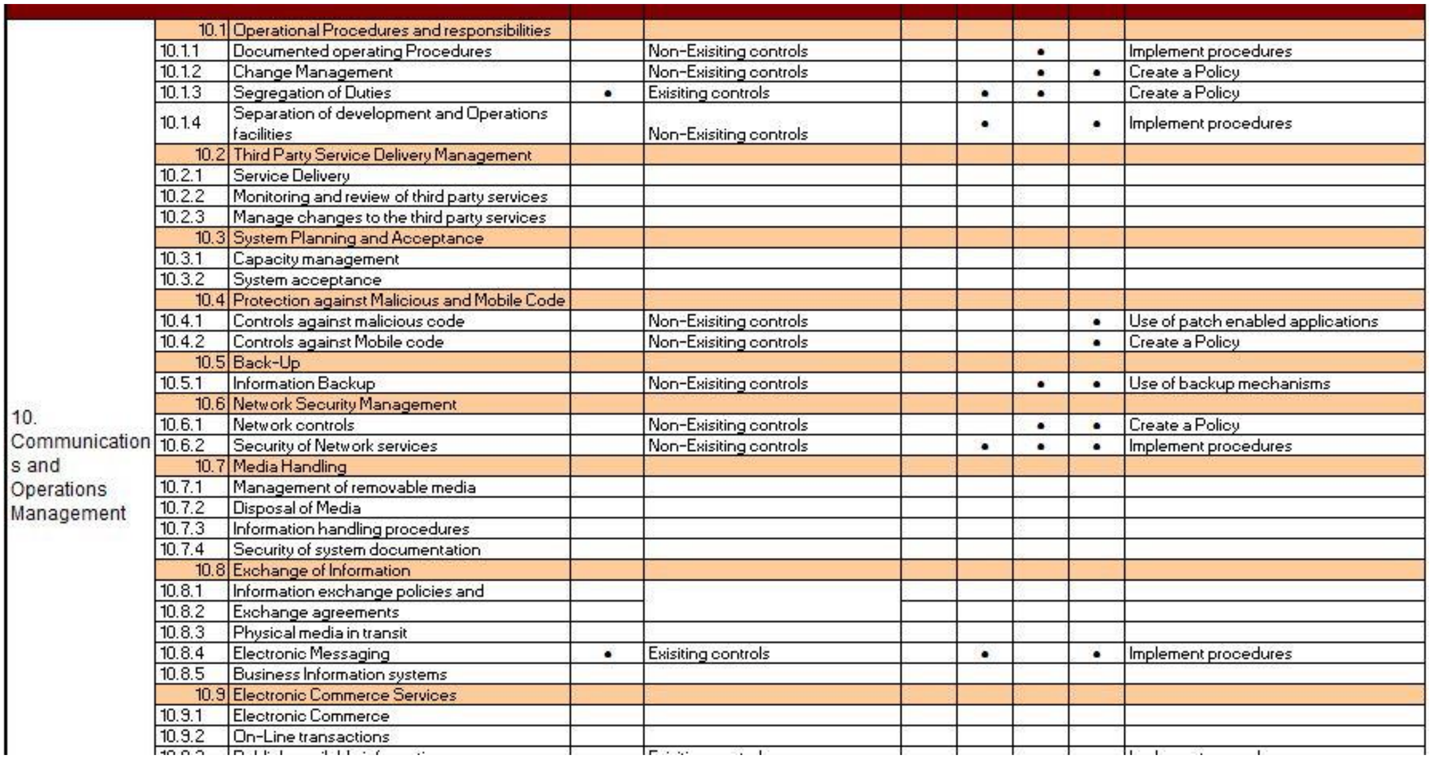
SOA



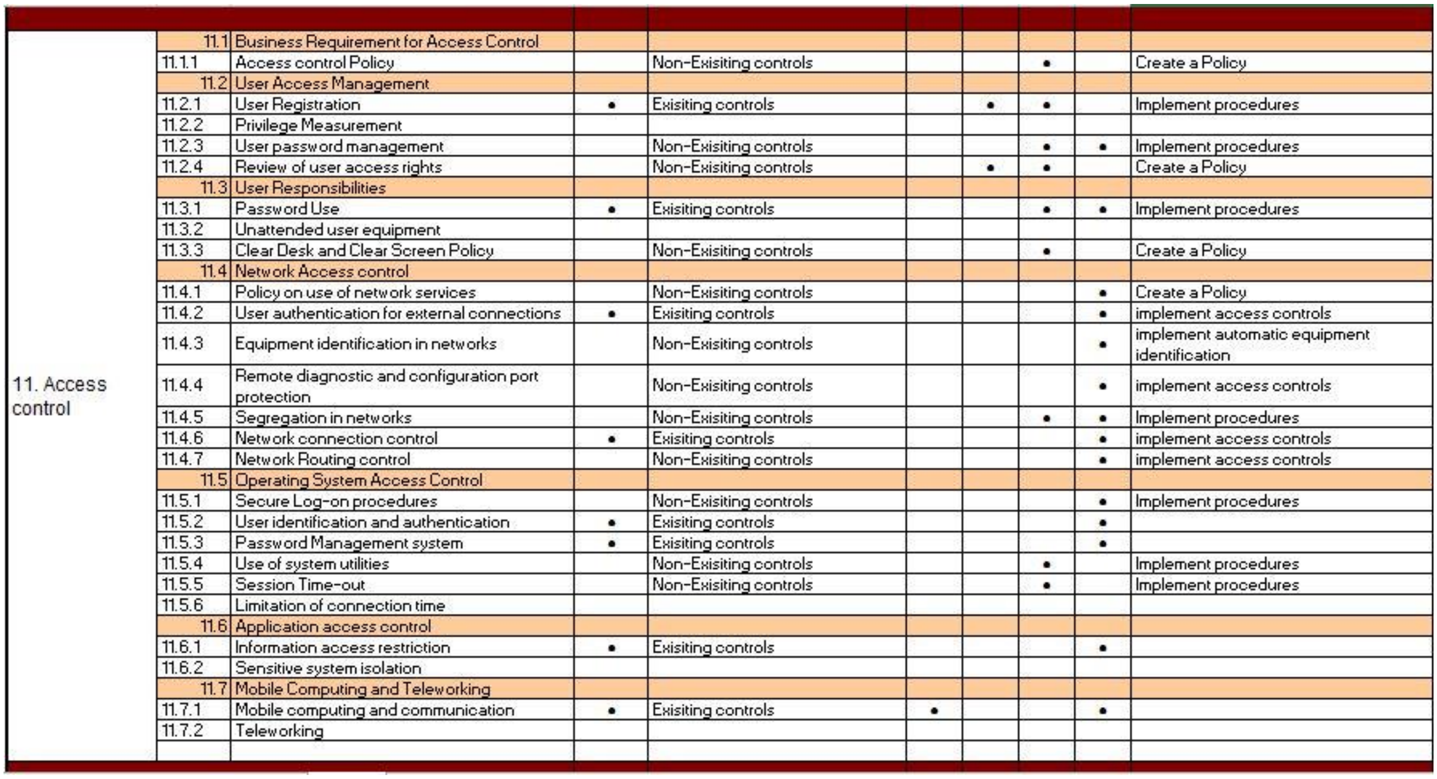
ISO 27001:2005 Controls			Current Controls	Remarks (Justification for exclusion)	Selected Controls and Reasons for selection				Remarks (Overview of implementation)
					LR	CO	BR/BP	RRA	
Clause	Sec	Control Objective/Control							
5. Security Policy	5.1	Information Security Policy							
	5.1.1	Information Security Policy Document		Exsiting Control			•		to protect the data
	5.1.2	Review of Information Security Policy							to prtect the data
6. Organization of Information security	6.1	Internal Organization							
	6.1.1	Management Commitment to information security							use information security provcedure
	6.1.2	Information security Co-ordination							
	6.1.3	Allocation of information security Responsibilities	•	Existing Control. Central Server has dedicated staff			•	•	
	6.1.4	Authorization process for Information Processing facilities							
	6.1.5	Confidentiality agreements							
	6.1.6	Contact with authorities							
	6.1.7	Contact with special interest groups							
	6.1.8	Independent review of information security							
	6.2	External Parties							
	6.2.1	Identification of risk related to external parties	•	Exsiting Control			•	•	keep logs
	6.2.2	Addressing security when dealing with customers	•	Exsiting Control			•	•	keep client details
	6.2.3	Addressing security in third party agreements							
7. Asset Management	7.1	Responsibility for Assets							
	7.1.1	Inventory of assets	•	Existing Control			•	•	
	7.1.2	Ownership of Assets	•	Existing Control	•		•		
	7.1.3	Acceptable use of assets	•	Existing Control			•		
	7.2	Information classification							
	7.2.1	Classification Guidelines							
	7.2.2	Information Labeling and Handling	•	Existing Control			•	•	



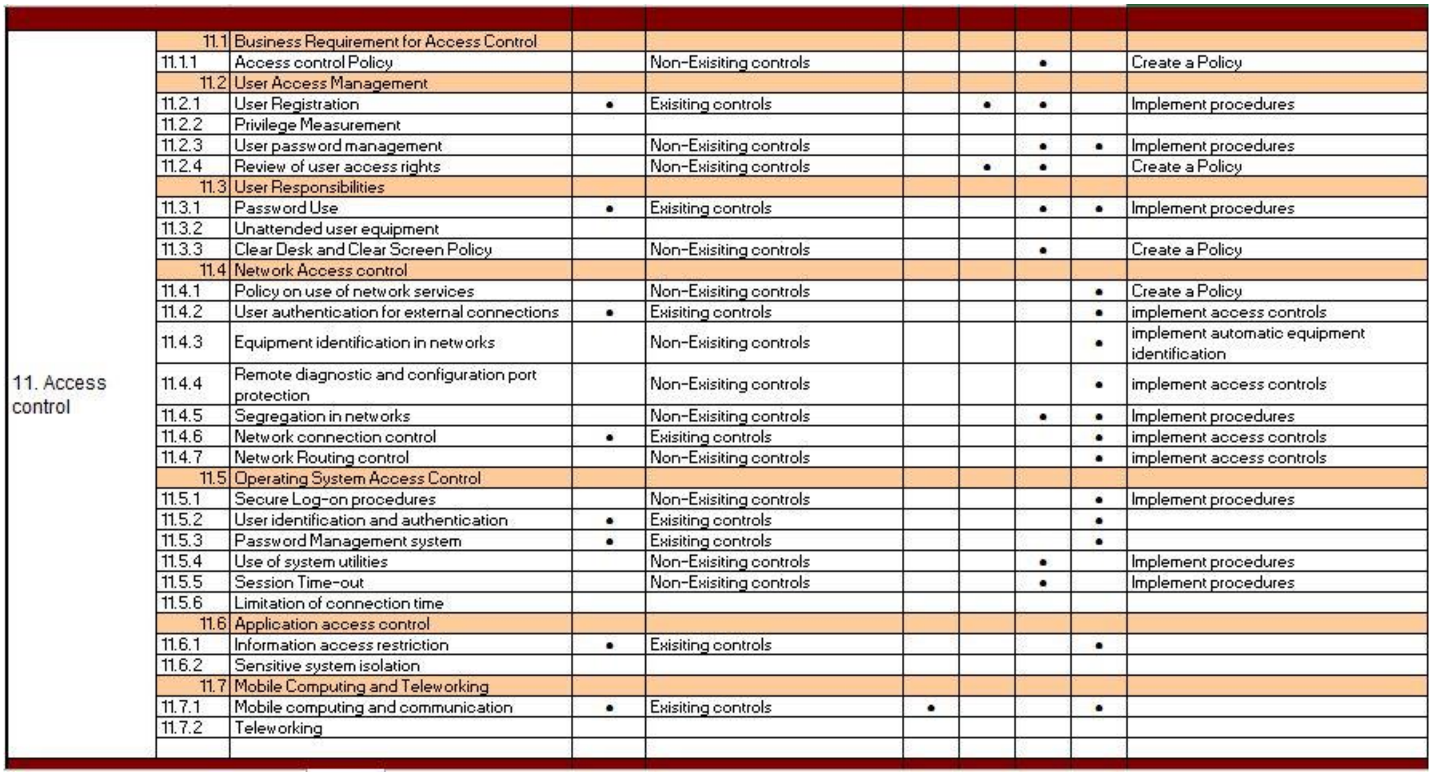
8. Human Resource Security	8.1	Prior to Employment							
	8.1.1	Roles and Responsibilities	•	Existing Control			•	•	assign dedicated staff for each roles
	8.1.2	Screening							
	8.1.3	Terms and conditions of employment	•	Existing Control	•		•	•	Policy created
	8.2	During Employment							
	8.2.1	Management Responsibility							
	8.2.2	Information security awareness, education and training	•	Exsiting Control			•	•	undergoing trainings
	8.2.3	Disciplinary process							
	8.3	Termination or change of employment							
	8.3.1	Termination responsibility							
	8.3.2	Return of assets							
	8.3.3	Removal of access rights		Non-Exisiting controls	•		•	•	
9. Physical and Environmental Security	9.1	Secure Areas							
	9.1.1	Physical security Perimeter							
	9.1.2	Physical entry controls	•	Existing controls		•	•	•	I established visitor control logs
	9.1.3	Securing offices, rooms and facilities	•	Existing controls				•	
	9.1.4	Protecting against external and environmental threats	•	Existing controls					
	9.1.5	Working in secure areas	•	Existing controls			•		Policy created
	9.1.6	Public access, delivery and loading areas	•	Existing controls					
	9.2	Equipment security							
	9.2.1	Equipment sitting and protection	•	Existing controls		•		•	
	9.2.2	Support utilities	•	Existing controls				•	
	9.2.3	Cabling security	•	Existing controls		•			
	9.2.4	Equipment Maintenance	•	Existing controls		•	•	•	Formalized PM mechanism
	9.2.5	Security of equipment off-premises	•	Existing controls					
	9.2.6	Secure disposal or reuse of equipment					•		Implemented procedure
	9.2.7	Removal of Property	•	Existing controls. Use of gate pass.					



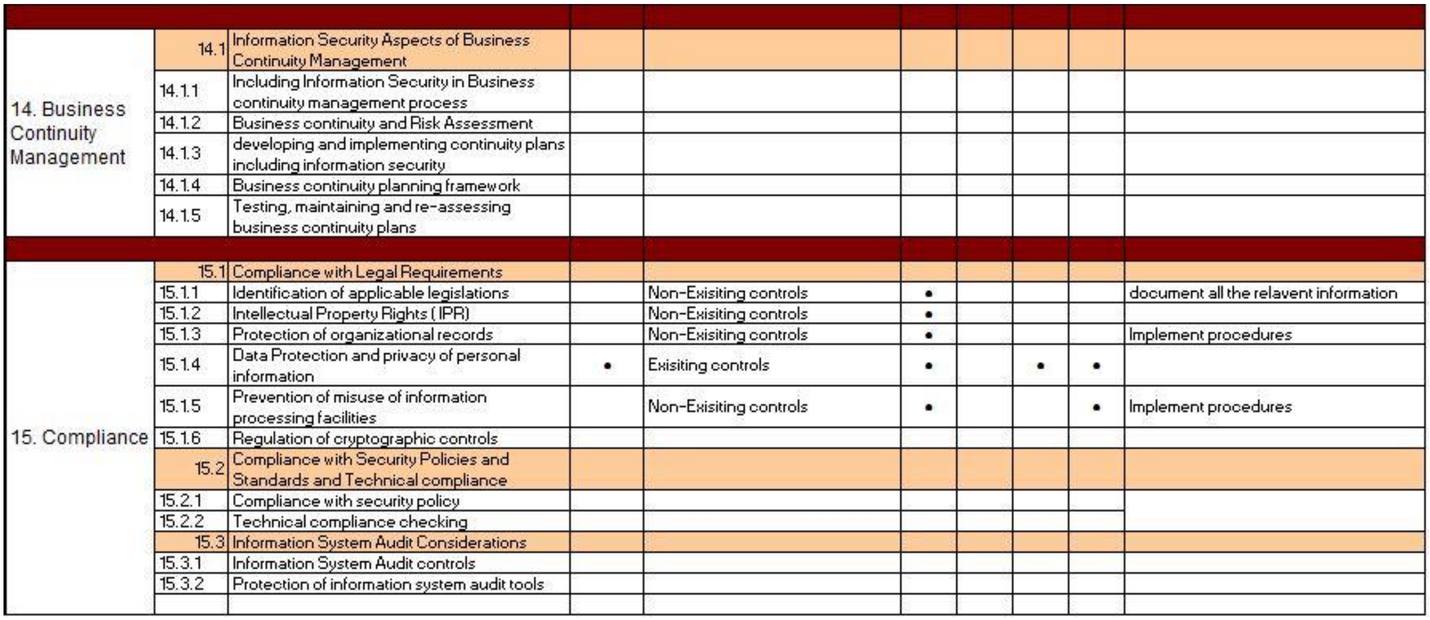
10. Communications and Operations Management	10.1	Operational Procedures and responsibilities							
	10.1.1	Documented operating Procedures		Non-Exisiting controls			•		Implement procedures
	10.1.2	Change Management		Non-Exisiting controls			•	•	Create a Policy
	10.1.3	Segregation of Duties	•	Exisiting controls		•	•		Create a Policy
	10.1.4	Separation of development and Operations facilities		Non-Exisiting controls		•		•	Implement procedures
	10.2	Third Party Service Delivery Management							
	10.2.1	Service Delivery							
	10.2.2	Monitoring and review of third party services							
	10.2.3	Manage changes to the third party services							
	10.3	System Planning and Acceptance							
	10.3.1	Capacity management							
	10.3.2	System acceptance							
	10.4	Protection against Malicious and Mobile Code							
	10.4.1	Controls against malicious code		Non-Exisiting controls				•	Use of patch enabled applications
	10.4.2	Controls against Mobile code		Non-Exisiting controls				•	Create a Policy
	10.5	Back-Up							
	10.5.1	Information Backup		Non-Exisiting controls			•	•	Use of backup mechanisms
	10.6	Network Security Management							
	10.6.1	Network controls		Non-Exisiting controls			•	•	Create a Policy
	10.6.2	Security of Network services		Non-Exisiting controls		•	•	•	Implement procedures
	10.7	Media Handling							
	10.7.1	Management of removable media							
	10.7.2	Disposal of Media							
	10.7.3	Information handling procedures							
	10.7.4	Security of system documentation							
	10.8	Exchange of Information							
	10.8.1	Information exchange policies and							
	10.8.2	Exchange agreements							
	10.8.3	Physical media in transit							
	10.8.4	Electronic Messaging	•	Exisiting controls		•		•	Implement procedures
	10.8.5	Business Information systems							
	10.9	Electronic Commerce Services							
	10.9.1	Electronic Commerce							
	10.9.2	On-Line transactions							



11. Access control	11.1	Business Requirement for Access Control							
	11.1.1	Access control Policy		Non-Exisiting controls			•		Create a Policy
	11.2	User Access Management							
	11.2.1	User Registration	•	Exisiting controls		•	•		Implement procedures
	11.2.2	Privilege Measurement							
	11.2.3	User password management		Non-Exisiting controls			•	•	Implement procedures
	11.2.4	Review of user access rights		Non-Exisiting controls		•	•		Create a Policy
	11.3	User Responsibilities							
	11.3.1	Password Use	•	Exisiting controls			•	•	Implement procedures
	11.3.2	Unattended user equipment							
	11.3.3	Clear Desk and Clear Screen Policy		Non-Exisiting controls			•		Create a Policy
	11.4	Network Access control							
	11.4.1	Policy on use of network services		Non-Exisiting controls				•	Create a Policy
	11.4.2	User authentication for external connections	•	Exisiting controls				•	implement access controls
	11.4.3	Equipment identification in networks		Non-Exisiting controls				•	implement automatic equipment identification
	11.4.4	Remote diagnostic and configuration port protection		Non-Exisiting controls				•	implement access controls
	11.4.5	Segregation in networks		Non-Exisiting controls			•	•	Implement procedures
	11.4.6	Network connection control	•	Exisiting controls				•	implement access controls
	11.4.7	Network Routing control		Non-Exisiting controls				•	implement access controls
	11.5	Operating System Access Control							
	11.5.1	Secure Log-on procedures		Non-Exisiting controls				•	Implement procedures
	11.5.2	User identification and authentication	•	Exisiting controls				•	
	11.5.3	Password Management system	•	Exisiting controls				•	
	11.5.4	Use of system utilities		Non-Exisiting controls			•		Implement procedures
	11.5.5	Session Time-out		Non-Exisiting controls			•		Implement procedures
	11.5.6	Limitation of connection time							
	11.6	Application access control							
	11.6.1	Information access restriction	•	Exisiting controls				•	
	11.6.2	Sensitive system isolation							
	11.7	Mobile Computing and Teleworking							
	11.7.1	Mobile computing and communication	•	Exisiting controls	•			•	
	11.7.2	Teleworking							



11. Access control	11.1	Business Requirement for Access Control						
	11.1.1	Access control Policy		Non-Exisiting controls			•		Create a Policy
	11.2	User Access Management							
	11.2.1	User Registration	•	Exisiting controls		•	•		Implement procedures
	11.2.2	Privilege Measurement							
	11.2.3	User password management		Non-Exisiting controls			•	•	Implement procedures
	11.2.4	Review of user access rights		Non-Exisiting controls		•	•		Create a Policy
	11.3	User Responsibilities							
	11.3.1	Password Use	•	Exisiting controls			•	•	Implement procedures
	11.3.2	Unattended user equipment							
	11.3.3	Clear Desk and Clear Screen Policy		Non-Exisiting controls			•		Create a Policy
	11.4	Network Access control							
	11.4.1	Policy on use of network services		Non-Exisiting controls				•	Create a Policy
	11.4.2	User authentication for external connections	•	Exisiting controls				•	implement access controls
	11.4.3	Equipment identification in networks		Non-Exisiting controls				•	implement automatic equipment identification
	11.4.4	Remote diagnostic and configuration port protection		Non-Exisiting controls				•	implement access controls
	11.4.5	Segregation in networks		Non-Exisiting controls			•	•	Implement procedures
	11.4.6	Network connection control	•	Exisiting controls				•	implement access controls
	11.4.7	Network Routing control		Non-Exisiting controls				•	implement access controls
	11.5	Operating System Access Control							
	11.5.1	Secure Log-on procedures		Non-Exisiting controls				•	Implement procedures
	11.5.2	User identification and authentication	•	Exisiting controls				•	
	11.5.3	Password Management system	•	Exisiting controls				•	
	11.5.4	Use of system utilities		Non-Exisiting controls			•		Implement procedures
	11.5.5	Session Time-out		Non-Exisiting controls			•		Implement procedures
	11.5.6	Limitation of connection time							
	11.6	Application access control							
	11.6.1	Information access restriction	•	Exisiting controls				•	
	11.6.2	Sensitive system isolation							
	11.7	Mobile Computing and Teleworking							
	11.7.1	Mobile computing and communication	•	Exisiting controls	•			•	
	11.7.2	Teleworking							



14. Business Continuity Management	14.1	Information Security Aspects of Business Continuity Management							
	14.1.1	Including Information Security in Business continuity management process							
	14.1.2	Business continuity and Risk Assessment							
	14.1.3	developing and implementing continuity plans including information security							
	14.1.4	Business continuity planning framework							
	14.1.5	Testing, maintaining and re-assessing business continuity plans							
15. Compliance	15.1	Compliance with Legal Requirements							
	15.1.1	Identification of applicable legislations		Non-Exisiting controls	•				document all the relavent information
	15.1.2	Intellectual Property Rights (IPR)		Non-Exisiting controls	•				
	15.1.3	Protection of organizational records		Non-Exisiting controls	•				Implement procedures
	15.1.4	Data Protection and privacy of personal information	•	Exisiting controls	•		•	•	
	15.1.5	Prevention of misuse of information processing facilities		Non-Exisiting controls	•			•	Implement procedures
	15.1.6	Regulation of cryptographic controls							
	15.2	Compliance with Security Policies and Standards and Technical compliance							
	15.2.1	Compliance with security policy							
	15.2.2	Technical compliance checking							
	15.3	Information System Audit Considerations							
	15.3.1	Information System Audit controls							
	15.3.2	Protection of information system audit tools							