SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Enterprise Standards and Best Practices for IT Infrastructure

(4th Year 2nd Semester 2016)

Lab Assignment

(ISO27k Statement of Applicability)

Name: Edirisinghe I.R

ID: IT12088560

Batch: Weekday

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	Yes	No Specific password policy document	■	□	■	□	Security Policy
	5.1.2	Review of Information Security Policy	Yes		□	□	□	□	
					□	□	□	□	
6. Organization of Information security	6.1	Internal Organization			□	□	□	□	
	6.1.1	Management Commitment to information security	Yes	Management have demonstrated their commitment to information security by the allocation of resources and investment in their people.	■	■	■	■	Management commitment
	6.1.2	Information security Co-ordination	Yes	Within the data center, all information security activities are co-ordinated.	■	□	■	■	Information Security forum
	6.1.3	Allocation of information security Responsibilities	Yes	All Staff need to fully understand their responsibilities and procedures related to information security	■	□	■	■	Roles And Responsibilities
	6.1.4	Authorization process for Information Processing facilities	Yes	A change request is required for any new processing facilities	■	□	■	■	Change Request Policy and Procedure

	6.1.5	Confidentiality agreements	Yes	Confidentiality Agreements for the protection of information are identified and regularly reviewed	■	■	□	□	Confidentially Agreement
	6.1.6	Contact with authorities	No	Unnecessary owing to scope of registration	□	□	■	■	
	6.1.7	Contact with special interest groups	No	Unnecessary owing to scope of registration (rely on automatic update for security and anti-virus protection)	□	■	■	□	
	6.1.8	Independent review of information security	Yes	This is conducted at least once a year by an internal/ external independent body.	□	□	■	■	Audit Procedure
	6.2	External Parties			□	□	□	□	
	6.2.1	Identification of risk related to external parties	Yes	External parties have access to the data centre.	■	□	■	■	Security in Third Party Agreements
	6.2.2	Addressing security when dealing with customers	yes	Customers have access to the data centre.	■	□	□	■	Dealing with Customer Access
	6.2.3	Addressing security in third party agreements	yes	Third party controls employed.	■	□	■	■	Security in Third Party Agreements
					□	□	□	□	
7. Asset Management	7.1	Responsibility for Assets			□	□	□	□	
	7.1.1	Inventory of assets	Yes	A record of all information assets are kept on-site	■	■	■	□	Risk Assessment ,Report And Asset ,Register
	7.1.2	Ownership of Assets	Yes	All assets in the scope of this registration are owned by the Technical Director.	■	□	■	□	Risk Assessment ,Report And Asset ,Register
	7.1.3	Acceptable use of assets	Yes	Acceptable use of assets is laid down in the policies & procedures of the system.	■	□	■	□	Acceptable Use of Assets

	7.2	Information classification			☐	☐	☐	☐	
	7.2.1	Classification Guidelines	Yes	All data is held electronically and is application specific	■	☐	■	☐	Information Handling
	7.2.2	Information Labeling and Handling	Yes	Impractical and unnecessary	☐	☐	■	☐	Information Handling
8. Human Resource Security	8.1	Prior to Employment							
	8.1.1	Roles and Responsibilities	Yes	All employees have job descriptions defining their roles and responsibilities.	■	☐	■	☐	Roles responsibilities
	8.1.2	Screening	Yes	Data centre standards require independent references be sought prior to commencement of employment.	■	☐	☐	☐	Screening.
	8.1.3	Terms and conditions of employment	Yes	All employees have Job security responsibilities included in their terms and conditions of employment	☐	☐	■	☐	Terms And Conditions
	8.2	During Employment			☐	☐	☐	☐	
	8.2.1	Management Responsibility	Yes	All applicable personal made aware of their responsibilities with regard to security	■	☐	■	☐	Roles and responsibilities
	8.2.2	Information security awareness, education and training	Yes	All staff receive on-site security training with regards to ISO27001 where needed		☐	■	■	Roles and Responsibilities
	8.2.3	Disciplinary process	Yes	All staff have been made fully aware of their responsibilities regarding information security	■	☐	☐	☐	Disciplinary Process
	8.3	Termination or change of employment			☐	☐	☐	☐	

	8.3.1	Termination responsibility	Yes	To prevent unauthorized access following termination of employment contract.	■	□	■	□	Termination Of Employment.
	8.3.2	Return of assets	Yes	To ensure return of all company assets	■	□	■	□	Return of Assets
	8.3.3	Removal of access rights	Yes	To ensure no unauthorized access following termination of employment contract.	□	□	□	■	User Access Management
9. Physical and Environmental Security	9.1	Secure Areas							
	9.1.1	Physical security Perimeter	■	Existing controls		■			
	9.1.2	Physical entry controls	■	Existing controls		■	■	■	Implement swipe card on all data centers and 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	Yes	AGS employees will follow appropriate operating instructions	□	□	■	□	Various Procedures/Police s as required by standard
	10.1.2	Change Management	Yes	Adopted as best practice.	■	□	■	□	Change control procedure
	10.1.3	Segregation of Duties	Yes	To prevent unauthorized modification of IT systems or abuse of position	□	■	■	□	Segregation of Duties
	10.1.4	Separation of development and Operations facilities	No	No development done at/by the Data Centre.	□	■	□	□	
	10.2	Third Party Service Delivery Management			□	□	□	□	
	10.2.1	Service Delivery	Yes	3rd party services are used	□	■	■	□	Contracts/SLA with providers
	10.2.2	Monitoring and review of third party services	Yes	Monitoring & review take place to ensure continuity of service	■	□	□	□	Security in Third Party Agreements

	10.2.3	Manage changes to the third party services	Yes	Managing changes to ensure continuity of service.	☐	■	■	☐	Security in Third Party Agreements
	10.3	System Planning and Acceptance			☐	☐	☐	☐	
	10.3.1	Capacity management	Yes	Growth is core to the business.	☐	☐	■	■	Capacity management
	10.3.2	System acceptance	Yes	To ensure all systems are acceptable prior to installation	■	☐	☐	■	Change control policy
	10.4	Protection against Malicious and Mobile Code							
	10.4.1	Controls against malicious code	Yes	Protection against malicious code	☐	☐	■	■	Malicious Code Protection
	10.4.2	Controls against Mobile code	Yes	System administrators has access to DMZ zones	☐	☐	■	■	DMZ zone
	10.5	Back-Up			☐	☐	☐	☐	
	10.5.1	Information Backup	Yes	To prevent the permanent loss of important information assets	☐	■	■	☐	Back-up Policy
	10.6	Network Security Management			☐	☐	☐	☐	
	10.6.1	Network controls	Yes	Safeguarding of information in networks	■	☐	☐	☐	Network Usage Policy
	10.6.2	Security of Network services	☐		☐	☐	☐	☐	
	10.7	Media Handling							
	10.7.1	Management of removable media			☐	☐	☐	☐	
	10.7.2	Disposal of Media			☐	☐	☐	☐	

	10.7.3	Information handling procedures	Yes	To ensure business continuity and prevent disruption	■	□	■	□	Information Handling
	10.7.4	Security of system documentation	Yes	Documentation held in both hard and electronic format	□	■	■	■	Security of System Documentation
	10.8	Exchange of Information			□	□	□	□	
	10.8.1	Information exchange policies and procedures	Yes	Contracts requirement	■	□	■	■	Information Exchange Policies and Procedures
	10.8.2	Exchange agreements	□		□	□	□	□	
	10.8.3	Physical media in transit	□		□	□	□	□	
	10.8.4	Electronic Messaging	Yes	All staff have access to a company e-mail account	■	■	■		Security in email documents policy
	10.8.5	Business Information systems	□				□		
	10.9	Electronic Commerce Services							
	10.9.1	Electronic Commerce			□	□	□	□	
	10.9.2	On-Line transactions	No	No E-commerce facilities used in ISMS	■	□	■	□	
	10.9.3	Publicly available information	Yes	All information has a security classification	□	■	■	□	Information Handling Policy
	10.10	Monitoring			□	□	□	□	
	10.10.1	Audit logging	□		□	□	□	□	
	10.10.2	Monitoring system use	Yes	Procedures have been developed for monitoring system use.	■	□	■	□	Event Logging and Monitoring System Use

	10.10.3	Protection of log information	Yes	Generated log information are well protected against tampering and unauthorized access	☐	☐	■	■	Event Logging and Monitoring System Use
	10.10.4	Administrator and operator logs	Yes	System/Database Administrator activities are monitored and logged	■	☐	■	☐	Event Logging and Monitoring System Use
	10.10.5	Fault logging	☐		☐	☐	☐	☐	
	10.10.6	Clock synchronization			☐	☐	☐	☐	
					☐	☐	☐	☐	
11. Access control	11.1	Business Requirement for Access Control			☐	☐	☐	☐	
	11.1.1	Access control Policy	Yes	For the protection of sensitive data and systems.	■	☐	■	■	Access control Policy
	11.2	User Access Management							
	11.2.1	User Registration	Yes	To prevent unauthorised access to information systems	■	☐	■	☐	User Registration
	11.2.2	Privilege Measurement	Yes	Certain positions carry privileges	■	☐	■	☐	Privilege Management Policy
	11.2.3	User password management	Yes	All applications need password protection	☐	☐	■	■	Privilege Management Policy
	11.2.4	Review of user access rights	Yes	Required to be reviewed periodically	☐	☐	■	☐	User Access Management Policy,
	11.3	User Responsibilities			☐	☐	☐	☐	
	11.3.1	Password Use	Yes	To ensure availability of systems	■	☐	☐	■	Privilege Management Policy
	11.3.2	Unattended user equipment	Yes	By User Equipment we mean the administrators' workstations.	■	☐	■	■	Clear Desk and Screening policy
	11.3.3	Clear Desk and Clear Screen Policy	Yes	Although assets are sited in a secure area, information	☐	■	☐	■	Clear Desk and Screening policy

	11.4	Network Access control			☐	☐	☐	☐	
	11.4.1	Policy on use of network services	☐		☐	☐	☐	☐	
	11.4.2	User authentication for external connections	☐		☐	☐	☐	☐	
	11.4.3	Equipment identification in networks	☐		☐	☐	☐	☐	
	11.4.4	Remote diagnostic and configuration port protection	☐		☐	☐	☐	☐	
	11.4.5	Segregation in networks	Yes	Networks segregated for the control of unauthorised access	■	☐	■	☐	Network Usage Policy
	11.4.6	Network connection control	Yes	To control access in accordance with the access control policy	■	☐	■	☐	Network Usage Policy
	11.4.7	Network Routing control	Yes	To prevent unauthorised access in shared networks	■	☐	■	☐	Network Usage Policy
	11.5	Operating System Access Control			☐	☐	☐	☐	
	11.5.1	Secure Log-on procedures	Yes	To control and manage user access	☐	☐	■	■	Password Management Policy
	11.5.2	User identification and authentication	Yes	To maintain records and monitor unauthorised activities	☐	☐	■	■	Password Management Policy
	11.5.3	Password Management system	☐		☐	☐	☐	☐	
	11.5.4	Use of system utilities	☐		☐	☐	☐	☐	

	11.5.5	Session Time-out	☐		☐	☐	☐	☐	
	11.5.6	Limitation of connection time	☐		☐	☐	☐	☐	
	11.6	Application access control			☐	☐	☐	☐	
	11.6.1	Information access restriction	Yes	A need to know policy is employed	☐	■	☐	■	Information Handling Policy
	11.6.2	Sensitive system isolation	Yes	All systems are treated as sensitive	☐	☐	■	■	Access Control Policy
	11.7	Mobile Computing and Teleworking			☐	☐	☐	☐	
	11.7.1	Mobile computing and communication	Yes	Used by system administrators to identify system failures and restart essential services after failure	■	■	☐	☐	Mobile Computing Policy
	11.7.2	Teleworking			☐	☐	☐	☐	
					☐	☐	☐	☐	
					☐	☐	☐	☐	
12. Information Systems Acquisition Development and Maintenance	12.1	Security Requirements of Information Systems			☐	☐	☐	☐	
	12.1.1	Security requirement analysis and specifications	☐		☐	☐	☐	☐	
	12.2	Correct Processing in Applications			☐	☐	☐	☐	
	12.2.1	Input data validation	☐		☐	☐	☐	☐	
	12.2.2	Control of internal processing	☐		☐	☐	☐	☐	
	12.2.3	Message integrity	☐		☐	☐	☐	☐	

	12.2.4	Output data validation	☐		☐	☐	☐	☐	
	12.3	Cryptographic controls			☐	☐	☐	☐	
	12.3.1	Policy on the use of cryptographic controls			☐	☐	☐	☐	
	12.3.2	Key Management			☐	☐	☐	☐	
	12.4	Security of System Files			☐	☐	☐	☐	
	12.4.1	Control of Operational software	Yes	To prevent unauthorised change control	☐	☐	■	■	Change control policy
	12.4.2	Protection of system test data	No	Data centre does not do any development maintenance or support of application system software	☐	☐	■	☐	
	12.4.3	Access control to program source library	Yes	Source code held as back up only .	■	☐	■	■	Backup Procedure
	12.5	Security in Development & Support Processes			☐	☐	☐	☐	
	12.5.1	Change Control Procedures	☐		☐	☐	☐	☐	
	12.5.2	Technical review of applications after Operating system changes	☐		☐	☐	☐	☐	
	12.5.3	Restrictions on changes to software packages			☐	☐	☐	☐	

	12.5.4	Information Leakage	Yes	Opportunities for information leakage need to be prevented	■	□	□	■	Access control policy
	12.5.5	Outsourced Software Development			□	□	□	□	
	12.6	Technical Vulnerability Management			□	□	□	□	
	12.6.1	Control of technical vulnerabilities			□	□	□	□	
					□	□	□	□	
					□	□	□	□	
13. Information Security Incident Management	13.1	Reporting Information Security Events and Weaknesses			□	□	□	□	
	13.1.1	Reporting Information security events	Yes	All security problems are notified to the Data Centre Manager.	□	□	■	■	Reporting Security Incidents Procedure
	13.1.2	Reporting security weaknesses	Yes	All security problems are notified to the Data Centre Manager.	■	□	■	■	Reporting Security Incidents Procedure
	13.2	Management of Information Security Incidents and Improvements			□	□	□	□	
	13.2.1	Responsibilities and Procedures			□	□	□	□	
	13.2.2	Learning for Information security incidents			□	□	□	□	
	13.2.3	Collection of evidence			□	□	□	□	
					□	□	□	□	

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	Yes	For on-going verification and validation of an effective approach to BCP	■	■	■	☐	Business Continuity Plan Test Policy
					☐	☐	☐	☐	
15. Compliance	15.1	Compliance with Legal Requirements			☐	☐	☐	☐	

	15.1.1	Identification of applicable legislations	☐		☐	☐	☐	☐	
	15.1.2	Intellectual Property Rights (IPR)	☐		☐	☐	☐	☐	
	15.1.3	Protection of organizational records	Yes	ISMS complies with industry, legal and contract	☐	■	■	☐	Compliance with Legal Requirements
	15.1.4	Data Protection and privacy of personal information			☐	☐	☐	☐	
	15.1.5	Prevention of misuse of information processing facilities	Yes	To ensure that all employees are aware of the policy on the use of company information processing facilities	☐	☐	■	■	Compliance with Legal Requirements
	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	Yes	Conducted by an Audit specialists to ensure compliance with security policies and standards	■	■	☐	■	Audit Compliance
	15.3	Information System Audit Considerations			☐	☐	☐	☐	

	15.3.1	Information System Audit controls	Yes	Internal audit team conduct regular audits of all policies and procedures adopted by the company to ensure effective implementation	☐	☐	■	■	
	15.3.2	Protection of information system audit tools	Yes	Controlled by IT manager to prevent misuse or compromise	☐	☐	■	☐	
					☐	☐	☐	☐	