SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

Enterprise Standards and Best Practices for IT Infrastructure

(4th Year 2nd Semester 2016)

Lab Assignment

(Information Security Risk Assessment)

Name: Edirisinghe I.R

ID: IT12088560

Batch: Weekday

Information Security Risk Assessment

Information asset	Known or suspected threats	Known or suspected vulnerabilities	Primary concerns (C/I/A)	Possibility of occurrence	Impact level	Raw risk level	Key information security controls in effect	Incident detectability	Detected risk level	Mean risk total	Comments, notes, explanation
Database X	Hacking	Internet connectivity; inadequate firewall protection	C + I	1	4	**4**	Data protection policies & procedures; network security controls; system security controls	3	**12**	**11**	
	Poor quality data	Poor quality information provided; incomplete checking and updating	A + I	3.5	2	**7**	Built-in integrity checks; routine procedures for checking & correcting data; ad hoc re-checks	2	**14**		
	Social engineering	Limited compliance with procedures; lack of awareness of the threat	C	0.5	3	**1.5**	Data protection policies & procedures; ongoing awareness program	4	**6**		
Web system Y	Hacking	Internet connectivity; inadequate firewall protection; web client	I + A	1	4	**4**	Network security controls; system security controls; data security controls	2	**8**	**12**	

	Social engineering	Limited compliance with procedures; lack of awareness of the threat	C	1	4	**4**	Data protection policies & procedures; network security controls; system security controls	4	**16**		
LAN	Hacking	Internet Connectivity, Inadequate firewall protection	C + I	1	4	**4**	Data Protection Policies, Network Security Controls	3	**12**	**16**	
	Virus, worm, Trojan or other malware	Internet Connectivity, Inadequate Virus Protection	C + I + A	3	2	**6**	Network security controls; system security controls; data security controls	3	**18**		
	Data or system corruption	Poor quality information provided, incomplete checking and updating	I + A	2	3	**6**	Data protection Policies, System Security Policies	3	**18**		
Backup tapes	Theft	No adequate protection	A	2	3	**6**	Password Protection, System Security Controls	4	**24**	**18**	
	Accidental or criminal damage, sabotage	No adequate protection	A	1	3	**3**	System Security Controls, Ongoing awareness program	5	**15**		
	Fire, flood	No adequate protection, Lack of awareness of thieves threat	A	1	3	**3**	System Security Controls, Ongoing awareness program	5	**15**		

PC's, laptops, PDAs etc. used by staff	Theft	No adequate protection, No password Protection	C + I	1	4	**4**	Password Protection, System Security Controls	5	**20**	**20**	
	Accidental or criminal damage, sabotage	No adequate Protection, No password Protection	C + I	1	4	**4**	System Security Controls, Ongoing awareness program	5	**20**		
Servers	Theft	No adequate protection, Server is centralized, No data encryption Techniques	C + I + A	1	4	**4**	System Security Controls, Ongoing awareness program	5	**20**	**30**	
	Accidental or criminal damage, sabotage	No adequate Protection, No password Protection, Lack of awareness of the threat	C + I + A	1	4	**4**	System Security Controls, Ongoing awareness program	5	**20**		
	Fire, flood	No adequate protection, No password Protection, Lack of awareness of the threat	C + I + A	1	4	**4**	System Security Controls, Ongoing awareness program	5	**20**		
Client information	Hacking	Only da central location store the data	I + A	1	4	**4**	system security controls; data security controls, Data protection policies & procedures;	2	**8**	**24**	
	Accidental or criminal damage, sabotage	Only da central location store the data	C	1	4	**4**	Data protection policies & procedures; system security controls	4	**16**		

Contract tenders	Hacking	Only da central location store the data	C+I+A	3	3	**9**	Data protection policies & procedures using system backups	3	**27**	**99**	
	Accidental or criminal damage, sabotage	Only da central location store the data	C+I+A	2	4	**8**	Data protection policies & procedures; system security controls	3	**24**		
	Data or system corruption	Only da central location store the data	C+I+A	4	4	**16**	Data protection policies & procedures; system security controls	3	**48**		