

# **Enterprise Standards and Best Practices for IT Infrastructure**

## **Lab Report**

### **Lab 04 - ISO27001\_Risk Assessment\_DOCUMENT**

**IT 120 62 966 – S.H.U.S.Wickramaratne**

**WEEKEND IT**



**Sri Lanka Institute of Information Technology**

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

**Specialized in Information Technology**

# Risk Assessment

Information asset	Known or suspected threats	Known or suspected vulnerabilities	Primary concerns (CIAA)	Possibility of occurrence	Impact level	Raw risk level	Key information security controls in effect	Incident undetectability	Detected risk level	Mean risk total
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	
Switches	Hacking	Internet connectivity; inadequate firewall protection	C+I	1	4	4	Network security controls; system security controls; data security controls	2	8	28
	Virus, worm, trojan or other malware	Internet connectivity; inadequate firewall protection	C+I	1	4	4	Network security controls; system security controls; data security controls	2	8	
	Data or system corruption	poor quality in administration or engineering the network	A+I	2	2	4	Higherarchical architecture for network administration and engineering. Privilege controls.	3	12	
Backup servers	Theft	poor physical security	C+I	1	4	4	CCTV cameras, security guards, controlled entrance.	1	4	12
	Accidental or criminal damage, sabotage	poor physical security, threatening	C+I+A	1	4	4	well trained security guards, link with the police station.	1	4	
	Fire, flood	Business situated in a low land or near a forest.	A	1	4	4	Fire distinguish methods, have a well maintained drainage system	1	4	
Servers	Accidental or criminal damage, sabotage	poor physical security, threatening	C+I+A	1	4	4	well trained security guards, link with the police station.	1	4	12
Cabling	Accidental or intentional Damage	Cables are lay across public area, Not shielded.	A	2	2	4	hide the cables, shield the cables.	3	12	24
	Corrosions	metal and copper cables	A	3	1	3	use fibre optics, shield the cables.	4	12	
Access points	Unauthorized access to the internet.	weak password and security.	A	2	1	2	strong password, monitor the usage.	2	4	18
	Hacking	Internet connectivity; inadequate firewall protection	C+I	1	4	4	Network security controls; system security controls; data security controls	2	8	
	Accidental or intentional Damage	Access points are not placed in a secure place.	A	2	1	2	place the access points inside a secured place.	3	6	
Operating system	Hacking	Internet connectivity; inadequate firewall protection; web client	C+I	1	4	4	Data protection policies & procedures; network security controls; system security controls	2	8	20
	Data or system corruption	poor quality in administration or engineering the system	A+I	2	2	4	Higherarchical architecture for system administration and engineering. Privilege controls.	1	4	
	Virus, worm, trojan or other malware	Internet connectivity; inadequate firewall protection	C+I	1	4	4	Network security controls; system security controls; data security controls	2	8	