Group No: 20

Name	Index no:
W.I.A.R.P.Fernando	16020251
M.A.W.Hansini	16020308
P.H.M.Nishadini	16020642
Sanduni Imalsha S.A	16020782

Risk Assessment

Organization: **University of Colombo School of Computing**

Goal: Provide education

Assets :

1. Stored files and database information
2. Network system
3. Examination information
4. Mail services
5. Financial System

Risk Matrix

	Consequences					
Likelihood	Doomsday	Catastrophic	Major	Moderate	Minor	Insignificant
Almost Certain				High (4)		
Likely			High (2)			
Possible			Extreme (1)			
Unlikely			Extreme (3)	High (5)		
Rare						

Risk Register

Asset	Threat / Vulnerability	Existing Controls	Likelihood	Consequences	Level of Risk	Risk Priority
Stored files and database information	Loss of information, theft, unauthorized modification	Firewall, policies	Possible	Major	Extreme	1
Network system	Attacks from hackers, system errors affecting the system, accidental fire	Layered firewalls and servers	Likely	Major	High	3
Examination information	Loss of information, theft, unauthorized modification	Firewall, policies	Unlikely	Major	Extreme	2
Mail services	Attacks, errors affecting system	Firewall, ext mail gateway	Almost certain	Moderate	High	5
Financial System	Unauthorized access, errors affecting system	Firewall, policies	Unlikely	Moderate	High	4

Risk treatment strategies for each asset

1. Stored files and database information
    - Data integrity
    - Data loss prevention
    - Protecting confidential data

2. Network system
    - Security; capture unauthorized access

3. Examination information
    - Data loss prevention
    - Protecting data
    - Data integrity

4. Mail services
    - Indicating spam emails

5. Financial System

Preventing from natural disasters(protecting financial information from disasters)
Data loss prevention
Protecting database from unauthorized people. (considering highly when sharing data)

Technological/organizational/operational measures of those assets

1. Measures

- Give users differentiated access permissions to the IT system.
- The internal organization should define the access permissions for each employee by means of an access permissions matrix.

2. Measures

- Keep data transfers from the intranet to the outside world via the Internet to an absolute minimum.
- Considering using the Transport Layer Security protocol (TLS) depending on the nature of the data that is to be processed.
- If staff or third parties outside the organization access the organization's intranet, a VPN should be set up.

3. Measures

- Staff should be authenticated each time they switch on their systems. The more sensitive the data they are processing, the higher the authentication requirements should be.

4. Measures
- Using spam detectors/filters.
- Using unique email format.

5. Measures

- Check whether the payments are completing on time in an accurate way. (mahapola, bursary, salary payments etc.)
- Doing Bill payments on time.