October 15

iLive Net (PVT)LTD

2017

This Report contains Risk analysis on critical assets and Countermeasure planes for iLive network(pvt)Ltd.

J.Tharjalan
IT15156570

iLive Network PVT Ltd

Annual Risk Report 2017

1. Introduction

iLive PVT Ltd is a famous Network company in srilanka That located in No 23, Carnival Mawatha Colombo 06. They have many branches across the country .But their headquartered in the Australia. iLive Network was approved by telecommunication regulatory commission of sri lanka[2].

This company was opened in srilanka on 25th December 2011.This company provides some major services to their customers that such as mobile network, Home broadband, iLive Television, Roaming Rates, Loyalty. And they are partnering with some man power company's also, for their call center services and teleshop services. This company has employees all over 45000 employees across the country.

2. Executive summary

This Section includes a summary of analyzing the critical information assets of this company, and identifying threats to that All assets and calculate the impact and finding the mitigating to that. The main framework is used for this report is OCTAVE Allegro[1] but, this is a hybrid framework. And the steps of the OCTAVE Allegro in the blow figure1. Mainly this framework will help to generate a unique report. It will give clear details about critical assets and Key issues. That will be in table 1.In the risk assessment criteria, do the evaluation on the potential threats. Then the threat profile contains what are the most effective threats available in the critical assets and how to mitigate them.After that summary and recommendation contain what are the new approach can take to avoid this kind of threats. And finally, there will be a calculation art that contains Anual cost detail, before mitigation and after mitigation. Then can find the safety cost amount. so it will help to maintain the proper maintenance on their assets and mainly they can avoid the harmful situations.

Key issues

Since they are dealing with large amount of customer services and maintain large data Centers so they have to maintain the security thing in that area because attack can be happened in physical manner or technical manner. So this is a very big challenge to marinating the security. If there is an attack occur that will give huge impact for this company. Since this is a internet service provider so they have to available for the all the time.

They have maintaining various type of servers for deferent services. That includes in the following table01. Risk management task is very effective task. Once we missed for the long time then it will be a big loss to the company. So the company have to do regular vulnerabilities scan to their critical information assets and prepare for the mitigation.

3. Technical Report

Risk assessment framework and functions.

We have used Octave Allegro as main framework and some other self-made operations for analyzing the risk assessment and impact.

Why Allegro Framework?

- First We need to find critical information of assets in this company.
- In this framework we have use top down approach methodology so a particular people have the ability to do the implementation part.
- Develop the risk measurement criteria whit organization mission.

Why self-made function?

- For the identify the risk analysis we have to do the quantitative risk analysis.
- In our threat profile we used some mathematical operations so that's why we created this functions.

Octave Phases can be define this following diagram.[1]

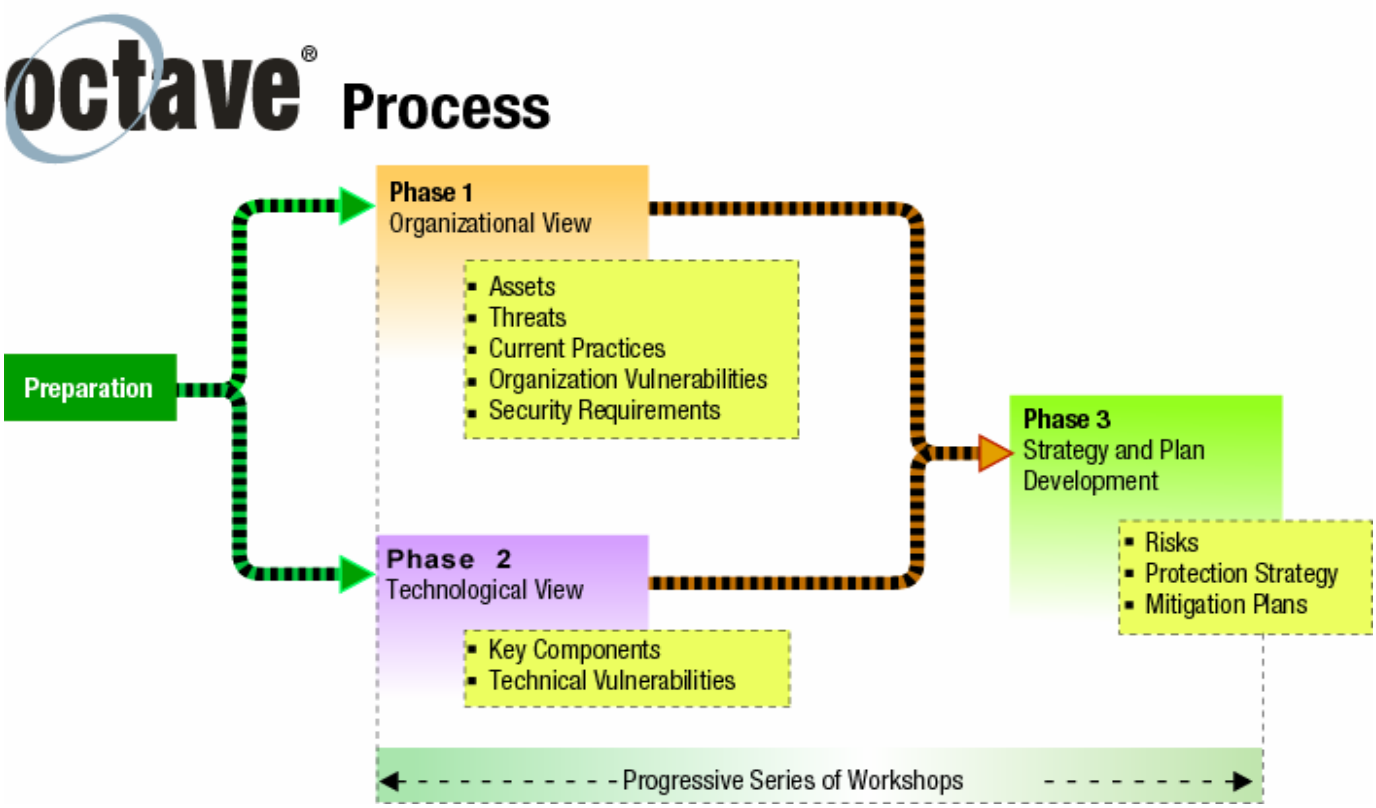

Figure 1

Risk assessment criteria

First finding the potential threats every threats has critical assets, so we have to prioritized them by companies risk tolerance level, financial things, and contains. We analyze the risk assessment report by evaluating these things.

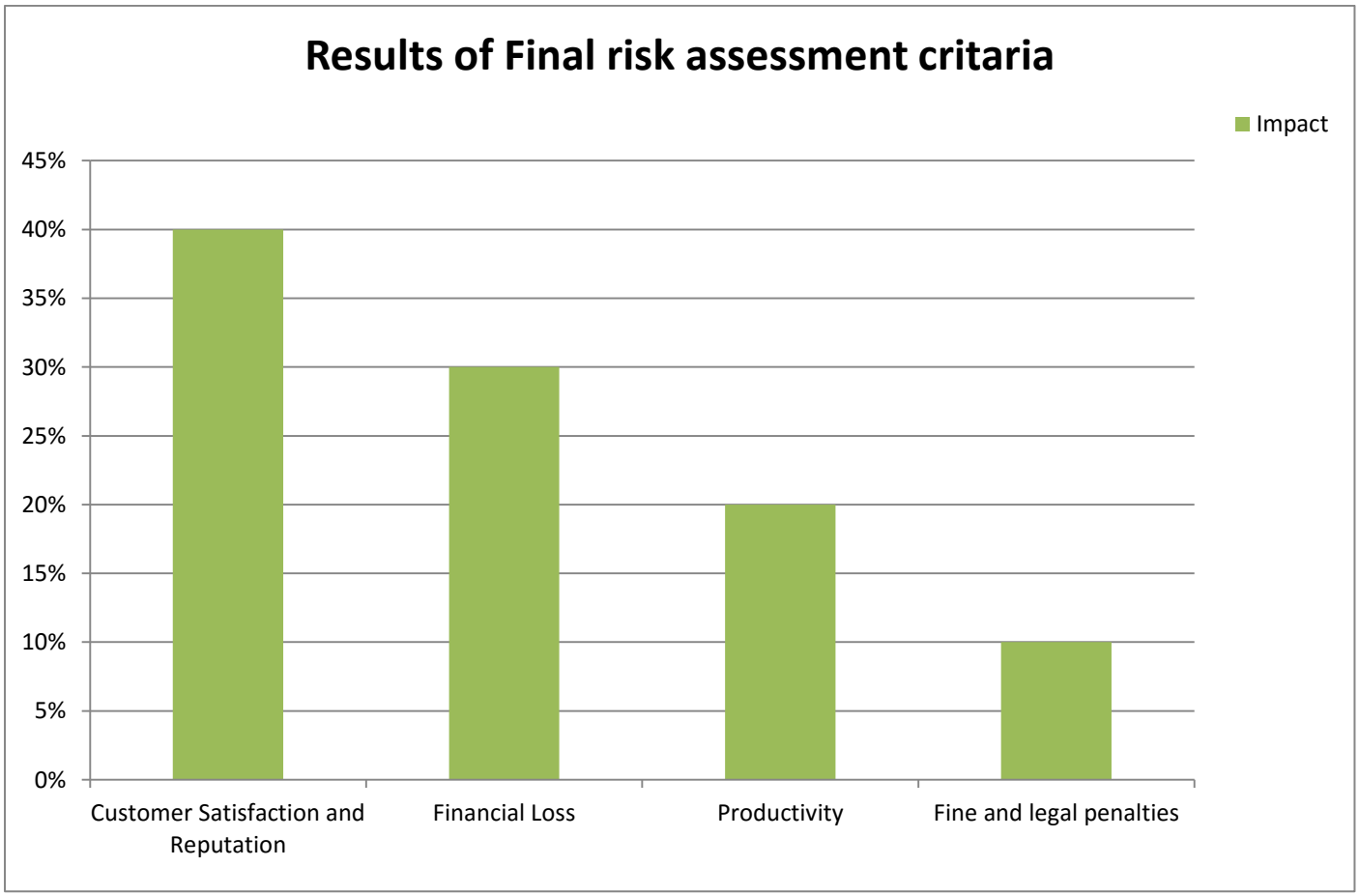

Figure 2

Organizational structure of iLive Network with various departments.

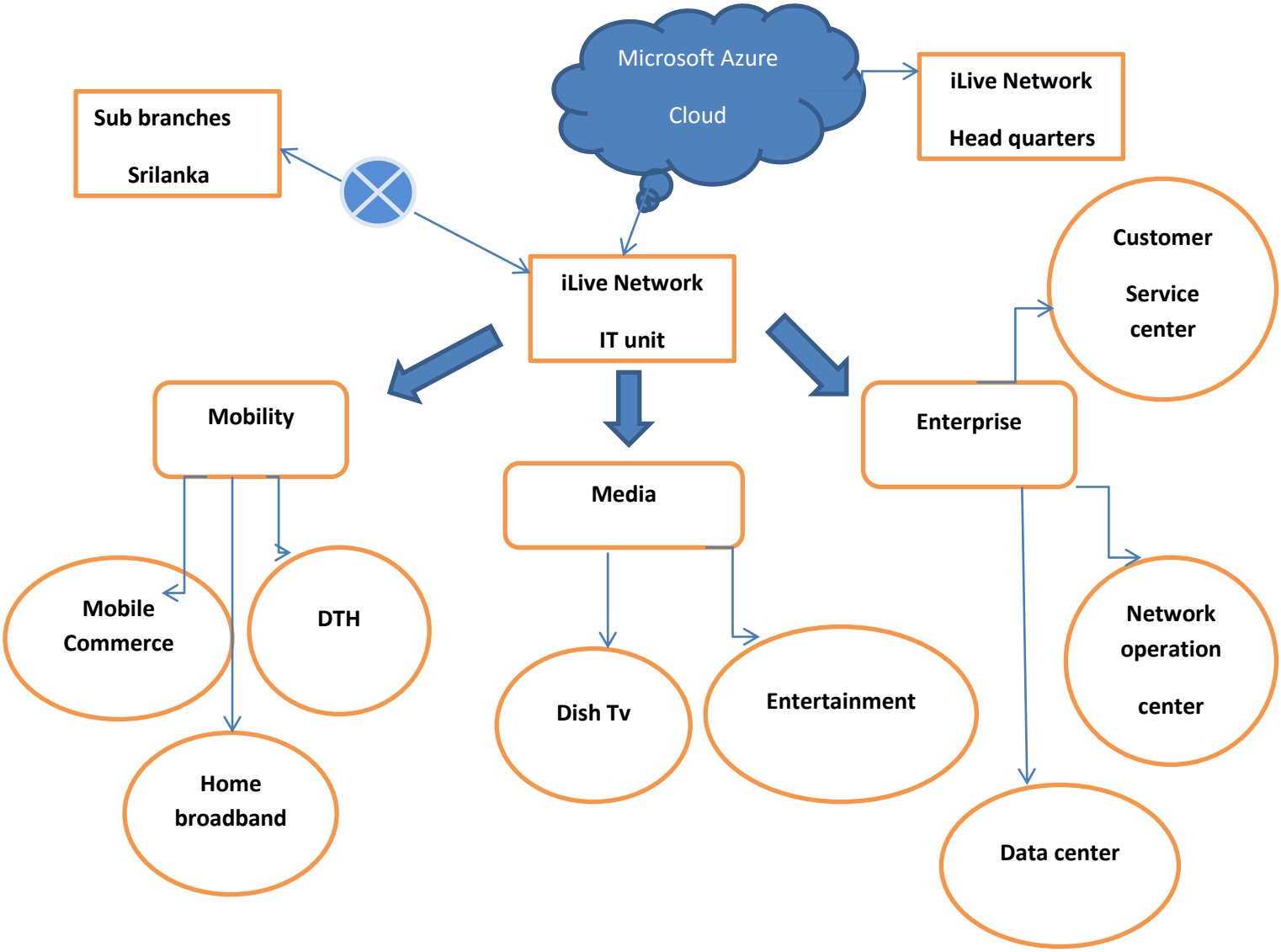

Figure 3

The above sector show how this company divided in to various departments how they interconnect with their main branches and their local sub branches. They provide main 3 services those are mobility, Media and Enterprises and using 3 deferent cloud computing for that . All the remote services are connect with their head office through the cloud basis server. And their branches also. And then all internal departments are connected through local area networks. In the main branch they have the central database that includes all the servers details . In the Risk analysis all the departments are connected through the iLive ITunit. This IT units will divides the clouds parts for three departments in above .This auditioning process will be done by some senior management official for each department. After analyzing we have found some critical assets. Headquarters always monitor their branches activities.

iLive Network PVT Ltd

Annual Risk Report 2017

Below sections shows critical assets of iLive network company that was identified through the risk assessment.

Critical Asset	Security Requirements	Description	Systems
ILive Pro Server	Integrity Confidentiality Availability	All group of their remote servers Are interconnected with this cloud.	Microsoft Azure (Cloud basic Serverless computing)
Real Time Connection[3]	Availability Integrity Confidentiality	All business and functions are depends on real time connections	**Meraki MX65W Cisco Router**
VPN Connections	Availability Integrity	This company has branches All over the world. So all The connections are through VPN.	**EDR-810** multiport secure router Express Vpn – company that provides Vpn services to this company
Administrative server	Integrity Confidentiality Availability	All the admin process and Customer financial status are Done through this server.	2xHp systems X320 M12 Windows 7 Enterprises
Internal Routers	Availability Integrity Confidentiality	This router are function as Bridge between internal And external networks. And Control the traffics as well.	**10x Cisco Catalyst 3560** Routers 5x switches
Data Center [4]	Integrity Confidentiality Availability	This centers includes all the Data about customers, systems Company secrets.	Cisco routers and switches NetApp storage systems (DataOTap) Cisco firewalls HP Blade servers
Backup Power	Availability	All the company depends on Electricity so when the power Is gone this backup will run Immediately.	Honda EB12D 12KW Silent Diesel Honda Ex10D

iLive Network PVT Ltd

Annual Risk Report 2017

Table01

Threat Profile of above critical assets.

Critical Assets	Threat	Impact Assessment	Mitigation Approach
ILive Pro Server	In Microsoft Azure Cloud system have some Threats such as Ease of use that Means malicious attacker can use Easily, secure data Transmission Data should be transmitted through SSL/TLS if not MITM attack will occur. Insecure API are accessible in internet So attacker can use token to gain customers details. Shared technology issues, Data Loss, Data breaches,	Impact for this vulnerabilities Is very high.bcouse if any of This vulnerabilities are exploited By attacker. Company will face Many problems because whole Company depends on this. And Connection will go down between All the branches. This will affect Integrity and confidentiality of this System.	-Stop sharing if account Credential between users Doesn't mater how trusted Partners. -Use single sign on -Implement end to end Encryption data -Use Up to date Systems In company system -Two factor authentication
Real Connectio	One of the main threats for the Connectivity is whether conditions, And since this company use **Meraki MX** Router for remote connection to their Sub branches. But this router has some Of the threats . it will allow remote Authenticated users to install particular Firmware by unspecified HTTP handler Access on their network. [3] And attacker can be do in physically also With the cable to serial ports. CVSS score for this was very high.	**Availability** impact is can shutdown all the system then an attacker can Easley make resources unavailable Legitimate users. **Integrity** impact is compromised total So this will be lost of system Protection after entire system will Compromised . **Confidentiality** impact is information Disclosure , result will all the system Details databases and financials status Being reviled or stolen. This will be huge loss to company.	Now there are update Patches are available So it can be fixed.
Admin Servers	Since this company used windows 7 As the main os to this administrator Server. So windows 7 has lots of Vulnerabilities to remotely access. So it Can be easily hijacking by attacker and Make changes to the data store and Make it as down.	Integrity will affect because if system Got compromised attacker can modify Because this is a admin server. And can make other system will not Available for the users.	They have to update The Operating system Best to preferred is Company can move to Linux environmental. This will be secure.
Data Center	There lots of threats in the data center Such as DDos Attacks,DNS Infrastructure Exploited, brute force attack when they Have week authentication, And here they are using NetApp Clustered Data OnTab this system has th vulnerabilities in the version of 9.0. attacker can get the passwords	When this vulnerabilities are used by The attacker this will give huge impact. When the DDos attack is happened All the data server got load after that They will go down then the all system Go down. And all of the customers passwords Will Get leak.	Application Delivery Controllers can be deployed In the center of the data center it will prevent form the unauthorized access to the applications

	information by logging of password entered by command line.[5]		
Backup Power	Honda EB12D 12KW Honda Ex10D Thi company use this 2 Backup generator's. this has some Heating problem and getting more Diesel to produce electricity	So when the company use it for a long Time this will get over heat and Consuming more diesel. Then some services of this company will not availal for at the time. This is will affect custom satisfaction and company will lose share	Company can change their Power plant source or the Can implement solar Panel.
VPN	Here they used **EDR-810** industrial Secure router for VPN remote access. This router has some critical exploitable Vulnerabilities and threats . when an Attacker accessing specific URL resource Locator on the web server then they can Access the system configuration log files. Attacker's low skill would able to Exploit This. So risk level is high[6]	If an attacker successfully exploited This vulnerability then he can escalate Privileges, and do the DDos attack. Then the company will face heavy blow.	-Put control system networks And remote devices behind the firewall ,and make them isolate from the company business network. -Update most current patch version

Table02

4. Summery & recommendations

First think have to do is update all the patches as mentioned above table . such as mainly they have to change the operating system of Admin Server because that was windows 7 system . so it should be change immediately to latest windows platform or most preferred in Linux environment. If they avoid it that will give big issue to the business by leaking customers credentials to unauthorized parties. Or They can change the configure settings to all the servers.

An for their storage and connectivity from headquarters they have use cloud serverless technology. To do that they have used Microsoft azure clod provider. Currently the cloud service has some threats those things are explained in the threat profile, so what they do is since it is a multi national company they have more competitors Now they have use shared cloud service with their partner company . that is a risk their all the details in the clod so if anything happened between this company and their partner company they can do some unauthorized work. To avoid that they can maintain don't share with 3rd party, and and use single sign on and two factor authentication technology form their cloud service provider.

Since they dealing with many services so the real time connection is very important thing so they have to maintain a proper way .now they use Meraki Mx series remote access router these are affected in the 2014 attack. So it can happen again so they have to update their patches for the regular time.

Never miss any patches, monitor all the device details.

Since they have no data back in this organization, if any natural disaster happen in the srilanka main center their srilankan business value will go down it will give affect their business. To avoid that they can maintain the simple backup plant that should be far way from the main center. So if anything happened workers go and continue the work so network never go down. They can find the 3rd party vendors to maintain their backup plant.

5. References

[1]2017. [Online]. Available: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf. [Accessed: 15- Oct- 2017].

[2]"Home - Telecommunications Regulatory Commission of Sri Lanka", *Trc.gov.lk*, 2017. [Online]. Available: http://www.trc.gov.lk/. [Accessed: 15- Oct- 2017].

[3]"Cisco Meraki Mx Firmware version 2014-09-24 : Security vulnerabilities", *Cvedetails.com*, 2017. [Online]. Available: https://www.cvedetails.com/vulnerability-list/vendor_id-16/product_id-30660/version_id-178269/Cisco-Meraki-Mx-Firmware-2014-09-24.html. [Accessed: 15- Oct- 2017].

[4]K. Cross, "The Top 5 Data Center Threats You Need to Know", *Infosecurity Magazine*, 2017. [Online]. Available: https://www.infosecurity-magazine.com/opinions/the-top-5-data-center-threats/. [Accessed: 15- Oct- 2017].

[5]"NetApp Support Community", *Kb.netapp.com*, 2017. [Online]. Available: https://kb.netapp.com/support/s/article/NTAP-20170630-0001?language=en_US. [Accessed: 15- Oct- 2017].

[6]"Moxa EDR-810 Industrial Secure Router Privilege Escalation Vulnerability | ICS-CERT", *Ics-cert.us-cert.gov*, 2017. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-16-294-01. [Accessed: 15- Oct- 2017].

Appendix

Exposure Factor (EF) : Percentage of asset loss caused by identified threat.
Single Loss Expectancy(SLE) = Asset Value * EF
Annualized Rate of Occurrence(ARO) = Frequency a threat will occur within year
Annualized Loss Expectancy = SLE *ARO
Safeguard Cost/Benefit = ALE before safeguard – ALE after safeguard – Annual Cost of safeguard

Assets Value

Microsoft Azure Cloud	:	45 00 000LKR
Meraki MX65W Cisco Router	:	2 00 000LKR
VPN and EDR 810 router	:	7 50 000LKR
HP systems X320 M12	:	4 50 000LKR
Cisco catalyst 3560	:	2 00 000LKR
NetApp Storage Systems	:	3 00 000LKR
Cisco Firewall	:	2 00 000LKR
HP Blade Servers	:	1 50 000LKR
Backup power	:	50 00 000LKR
Windows premium	:	50 000LKR
Monthly Cost	:	50 00 000LKR

Admin server :

Before Mitigation

EF = 20%
SLE = (450000 + 50000)*20%
= 100 000 LKR
ARO = 5
ALE = 100 000* 5
= 500 000 LKR

After Mitigation

EF = 13%
SLE = (450000+50000)*13%
= 65000 LKR
ARO = 5
ALE = 65000*5
= 325000

Annual Cost of safeguard = 80000
Safeguard Cost = 500000 - 325000 - 80000
= 95000LKR

iLive Network PVT Ltd

Annual Risk Report 2017

Real Time Connectivity :
Before Mitigation

EF = 10%
SLE = (200000)*10%
= 20 000 LKR
ARO = 5
ALE = 20 000* 5
= 100 000 LKR

After Mitigation

EF = 5%
SLE = (200000)*5%
= 10000 LKR
ARO = 5
ALE = 10000*5
= 50000 LKR

Annual Cost of safeguard = 25000
Safeguard Cost = 100000 - 50000 - 25000
= 25000LKR

Microsoft cloud Azure :
Before Mitigation

EF = 20%
SLE = (45 00 000)*20%
= 900 000LKR
ARO = 5
ALE = 900 000* 5
= 4500 000 LKR

After Mitigation

EF = 5%
SLE = (45 00 000)*5%
= 225000 LKR
ARO = 5
ALE = 225000*5
= 1 125 000 LKR

Annual Cost of safeguard = 100000
Safeguard Cost = 4500 000 - 1 125 000 - 100000
= 4275000LKR