**Muni University**

**BACHELOR OF INFORMATION SYSTEMS**

Year 3, Semester 2

Course Name: **IT Security & Risk Management**

Course Code: **ISM 3201**

Lecturer: **NKAMWESIGA Nicholas**

Group 2: **Project Assignment**

**Back ground information**

**As part of the Requirements in fulfillment of conditions for graduation in bachelors of information systems the department of computer and information systems through the lecturer of IT risks and information has assigned the students to conduct IT risk assessment in various departments in Muni University. This is entirely an academic activity.**

**The questionnaires below are meant to fulfill the demands of the course unit. Would you kindly cooperate in filling the questionnaire which will give basics for report writing for your department.**

**GOVERNANCE**

**Governance 1**

Question 1: Does the board of governors(senate) issue policy statement on information security?

a. yes, they do

b. they do but take long to update the policy

c. I am not sure

d. no they don't

Question 2: If policy statement is issued, does it( tick all correct statements)

a. recognize information as a vital business asset

b. acknowledge information risk management as business enabler

c. contain the boards acceptance of ultimate accountability for information risk management

d. assign management and employees security responsibilities

e. not sure

**Governance 2**

Question 1: Does the server room have a senior management committee to coordinate information risk management?

a. Yes well coordinated

b. Yes coordinating team

c. I will find out

Question 2: Does each head of department assume responsibility for their named information assets or its a sole responsibility of the server room?

a. Yes

b. No

c. That was not clearly stated in policy

Question 3: Does the server room have trained staff(s) specifically for security roles?

a. Yes but he or she is also assigned other roles

b. Yes he or she is only tasked with security roles.

c. No the server room is always secured.

**Governance 3**

Question 1

Does the muni server room have a suitable information risk policy to address threat sources and actors, prioritize risks, manage information risks during the systems development, acceptance , operational and decommissioning?

a. yes

b. no we just act

c. not sure

**Governance 4.**

Question 1: Do you usually organize security awareness, education, and training for the staff and students?

a. yes, every month

b, yes every semester

c. yes every academic year

d. yes for new entrance

e. no all staff and students are aware of security implications.

Qtn2: Are there penalties for breaching of security rules by a staff or student?

a. yes

b. No

c. Not sure

**Governance 5**

Question 1: Does the server room have an appropriate business continuity and disaster recovery programs?

a. yes, frequently updated

b. yes but takes long to be updated

c. no the server room is always safe

d. am not sure

**Governance 6.**

Question 1. Are the operation of the server room in compliance with NISF (National Information Security Policy)?

a. yes

b yes but other security frameworks are considered like …………………

c. no we just do our work

d. I will find out.

**INFORMATION SECURITY**

**IS 1**

**Question 1:** is there a definitive register of business critical facilities, systems , sites, and network associated with server room.

A yes well kept

b. yes

c. Am not sure

d. No we just do our work

Question 2: How often is the asset register auditor?

a. less than a month

b. every two month

c. not sure of the frequency

d. I don’t know

**IS 2.**

**Question 1.** while sharing or allowing connections to the computer assets, do you employ cryptographic solution to produce users and applications the underlying trust to operate authentication, integrity,confidentiality, and repudiation security sevices.

a. yes, all our systems are secured.

b. yes in some computer assets

c. no muni university has no hackers

Question 2. if yes which cryptographic cyphers or tools do you use?

(i)…………………………………………….

(ii)…………………………………………….

(iii)……………………………………………

(iv)……………………………………………

**IS 3**

Question 1: while acquiring new server room computer assets, do you ensure that suppliers are subject to and pass a national security impact assessment?

a. yes but not always

b. yes always as this is a government university

c. I will find out

d. no just pay.

Question 2: if yes how often do you assess compliance of suppliers?

a. only during the first acquisition.

b. every acquisition

c. I am not sure

Question 3 after acquiring server room computer assets, do you first test them before deploying them in production?

a. No we trust our suppliers

b. Yes but not for all acquisition.

c. yes we always

IS 4

Question 1. do applications associated with server room like module use the principle of least privilege and the need to know principle?

a. yes but not all applications

b. yes all applications do

c. no our applications work well

d. I am not sure what least privilege and the need to know principle are about.

Question 2. which access control model do you employ for the main server.

a. discretionary access control model

b. role based access control model.

c. mandatory access control model

d. all the above

e. non of the above

f. we don’t have hackers within the university.

Question 3. which of the following password management techniques (systems) do you use?

a. password synchronization

b. self service password reset

c. assisted password reset

d. legacy single sign on

e. we don’t use any of the above

f. am not sure what all these are about

IS 5

Question 1. Are your networks segregated (zoned) across various departments?

a. yes all departments have independent network.

b. yes but its only administration that has independent networks.

c. no we only have one network.

Question 2. Are network intrusion detection (NIDS) and network intrusion protection (NIPS) installed in your networks?

a. yes but only Network intrusion detection devices

b. yes but only network intrusion protection devices.

c. yes both of them

d. no we don’t have hackers in muni university.

IS 6

Question 1. Does the server room have malicious code policy (that require installation of anti-virus or anti malware software, updates of anti-viruses or anti-malware software signatures, system scanning , etc)?

a. yes all these are in place

b. yes but some of them

c. no all our systems run on linux

Question 2. Does your server identify and block all direct access eg email attachments, social media, malicious websites and indirect access eg unauthorized personal laptops, PDA, USB, CD/DVD routes that threat actors could use to inject malicious codes?

a. yes all these are in place

b. yes but some

c. not yet, we haven’t had any issues

IS 7.

Question 1. Is the hard drive on which the server operating system is running encrypted?

a. no but we intend to do that in the near future.

b. no since no one has access to the server room

c. yes including even BIOS password

d. yes only the hard drive is encrypted

Question 2. Do you use privately owned devices on the server?

a. yes only during emergencies

b. yes if its only available option

c. yes our devices are safe

d. no the security policy doesn’t allow that.

IS 8

Question 1: Is there restriction to any one outside accessing the internal networks?

a. no any one using computer can access

b. yes but through passw0rd restrictions.

c. some networks are freely available

d. not clear

IS 9

Question 1. How often are users and system logs audited?

a. only when there is an issue

b. usually in less than a month

c. usually in more than a month

d. we don’t really have any pattern that we following

IS 10

Question 1. Do you carryout backups

a. yes

b. no

Question 2. If yes for question 1 answer the following

which type of backup do do you carryout

a. full backup

b. differential backup

c. both a and b

d. we don’t really follow any pattern

Question 3. what is the frequency of your backup

a. daily

b. weekly

c. in a fortnight

d. monthly.

e. more than a month

f. we don’t follow any pattern

Question 4. Are your backups on-site or off-site

a. yes

b. no

Question 5. Is a periodic inventory taken to verify that the appropriate backup files are being maintained?

a. Yes

b. No

PERSONAL SECURITY.

Question 1. In case of any disaster occurrence, are the server room staff insured against injuries

a. yes but not all of them

b. yes all of them

c. no you just get your pay

d. Am not sure

PHYSICAL SECURITY.

Question 1. Which physical devices are used to identify and allow access to server room by the staff?

…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

Question 2. Does the university have any policies for temporary access by employees, visitors or outside vendors (e.g. are these individuals escorted during the activities or are badges or sign-in logs used)?

a. yes

b. no

**Thank you for your kind responses.**

Transforming lives

The end.