Muhammad Izham Bin Norhamadi
B032020039

No: .... Date: ....

Question 1

a) A company personnel that reports to management or the audit committee of board of directors

b) Process of evaluating the potential risks in an organization's information systems.

c) Involves the identification and assessment of the level of risk, calculated from the values of assets, threats to assets, and their vulnerabilities and likelihood of exploitation

d) i. Database server
   - hardware
   - Data center

ii. Application server
   - hardware
   - Server room

iii. Web server
   - software
   - Server room

iv. Routers
   - network device
   - Central network

Muhammad Izham Bin Norhamadi
B032020039

No: .... Date: ....

e) i. 1) Steal sensitive data
2) Inject malicious program in systems

ii. 1) Accidental policy violation
2) Disgruntled employee sabotaging

iii. 1) Reduce in revenue
2) Decrease trust in business partnership

iv. 1) Misconfigured web server
2) Single point of failure

v. 1) Destruction of assets
2) Attract cybercriminals

f) i. Complete system failure
- A critical system failure will stop most operations in the information systems

ii. Data theft
- Stolen sensitive data will put a risk in organization but will not affect operations.

iii. DDoS attack on web server
- IPS and Firewall will mitigate DDoS attack

STANDARD

Muhammad Izham Bin Norhamadi
B032020039

No: ....

Date: ....

g) i. Unprotected critical asset from natural disaster
Recommendation : Surround or move critical assets to protected area with walls

ii. Server failure causing loss of data
Recommendation : Define disaster recovery plan and backup schedule for servers

iii. Unauthorized access to sensitive data
Recommendation : Protect data with authentication system with set of roles

h) - Risk elimination :
- Create backup schedule for critical systems

i) - Risk reduction
- Set vpn configuration to access organization's network with employee's credentials

j) - Application server failure
- Router failure
- Database failure

STANDARD

Muhammad Izham Bin Norhamadi
B032020039

No: ....

Date: ....

Question 2

a) i. the process to determine and evaluate the potential effects of an interruption to critical business operations as a result of disaster, accident or emergency

ii. document that consists of critical information an organization needs to continue operation during unplanned events.

b) i. AV = RM 10,000,000

ii. EF = 0.25

iii. SLE = AV * EF
= 10 000 000 * 0.25
= RM 2 500,000

iv. ARO = 5/2 = 2.5

v. ALE = 2 500 000 * 2.5
= 6 250 000

Muhammad Izham Bin Norhamadi

B032020039

No: .... Date: ....

c) i. RM 50,000

ii. ARO = 1

iii. RM 250,000

iv. 80%

v. $250\,000 * (80/100)$

$= 200000$

vi. $\text{ROI} = \dfrac{250\,000 - 200\,000}{50\,000} \times 100$

$= 100\%$

vii. $200000 * 1$

$= \text{RM } 200000$

~~viii. Yes, because the expected loss from a single attack is greatly reduced when the control is implemented, saving more money than the cost of the program.~~

viii. Yes, because for the cost of RM 50,000 of implementing control, the organization can save as much as RM 200,000 annually

Muhammad Izham Bin Norhamadi
B032020039

No: .... Date: ....

Question 3

a) ISMS defines and manages controls that an organization needs to implement to ensure that it is sensibly protecting the confidentiality, integrity and availability of assets from threats and vulnerabilities

b) ISO 27002 establish guidelines and general principles for starting, implementing, maintaining and improving the management of information security in an organization.

c) 1) Secure information and assets
- An ISMS helps protect digital information including intelectual property, company secrets, and personal information

2) Increase resilience to cyber attack
- An ISMS helps respond to evolving security threats

d) ISO 27001 focuses on information security risks while ISO 31000 include other type of risks such as market

e) 1) Inital certification audit
2) Periodic surveillance audits
3) Re-certification every 3 years

f) Plan - Establishing the ISMS
Do - Update and improvement of ISMS
Check - Monitor and review ISMS
Act - Implement and workings of ISMS

STANDARD

Muhammad Izham Bin Norhamadi
B032020039

No: .... Date ....

g)
- Risk avoidance
- Risk reduction
- Risk transfer
- Risk acceptance

h) IT auditor helps organizations by protecting their internal controls and data witthin their technology system.

STANDARD