COMP60721

Two hours

Please use a ruler for diagrams and tables

Do NOT use lists without an explanation of each element in the list.

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

IT Governance

Date: Monday 25th January 2016

Time: 14:00 - 16:00

Please answer any THREE Questions from the FIVE Questions provided

---

This is a CLOSED book examination

The use of electronic calculators is NOT permitted

[PTO]

1 RESPONSIBILITY

a) Give 5 definitions of IT Governance (5 Marks)

b) Why is good governance a prerequisite for security? (4 marks)

c) The IT department of a bank has the technical know-how and the budget to implement encryption technologies to protect the transmission of a customer's transactions between a PC and the bank's systems.

Who needs to be involved to make this security technology an enabler not a hindrance? (5 marks)

d) How can the opinions of the different stakeholders be collected and synthesised into a set of managed requirements? Comment on the strengths and weaknesses of different methods. (6 marks)

2 STRATEGY

a) List 5 risks of using public networks to transmit sensitive information. (5 marks)

b) List a countermeasure that can treat each of these risks. Make it clear which countermeasure applies to which risk. (5 marks)

c) Explain the importance of strategy to the governance of an information system. Focus on the achievement of an adequate level of security. (3 marks)

d) ABC Corporation is changing its business model. They had previously had their own sales team but have replaced it with a network of resellers and an on-line shop for customers' self-service.

What are the implications of this change on the security of its business data? (1 mark)

Describe who is involved (from the points of view of accountability and responsibility, and who is consulted or just informed). (2 marks)

Sketch out - in a labelled diagram – the architecture of a likely information system: its components, its stakeholders, and interfaces where security is most at risk. (4 marks)

[PTO]

3 ARCHITECTURE/STRATEGY AND ACQUISITION

a) How can cloud computing improve security? (4 marks)

b) Explain how security may be managed through the supply chain. (4 marks)

c) The Ruritanian Oxygen Company (ROC) supplies medical gases (such as oxygen in cylinders) to hospitals and patients at home. When a patient leaves a hospital, the hospital will order a supply from ROC for the patient. That supply is then renewed through the patient's general practitioner. ROC operates a network of warehouses and fleet of vans who collect empty cylinders, refill them, and deliver them to the patients. Patients may delegate the ordering of new cylinders to someone else. ROC does not have the capacity to supply the whole country so it will subcontract the supply to local medical gas companies when necessary. It currently uses an information system based on printed forms and facsimile machines but would like to upgrade it to a system where it can track its vans and send them new orders without the drivers having to return to the depot to collect instructions.

Suggest a typical dataset that is required to ensure the uninterrupted supply of medical gases to the patients. Divide this dataset into business impact levels.

(4 marks)

Design – in a well-labelled diagram - the information security architecture that will support the confidentiality, integrity, and availability of the information handled during the process of supplying the medical gases.

(6 marks)

At what points will non-repudiation be important?

(1 mark)

Build a business continuity process into your design.

(1 mark)

4 PERFORMANCE

a) The cells in the table below are scrambled. Match each Status (in the second column) with its relevant maturity level (shown in the first column). Explain the meaning of each level of maturity.

Level	Status
0	Optimizing
1	Quantitatively Managed
2	Incomplete
3	Managed
4	Performed
5	Defined

(5 marks)

b) What is the difference between leading and lagging metrics? Give examples.

(2 marks)

c) How can leading and lagging metrics be turned into a real-time tool for IT governance? What decisions could the tool support?

(5 marks)

d) Company B handles sensitive, personal medical data and has decided to outsource the provision of its IT to Company Z. Company Z has proposed a service comprising:

- Data back-up
- Remote desktop support
- On-site back up
- Antivirus
- Annual review and recommendations for improvement.

How can the performance of these proposed elements be measured and monitored?

(3 marks)

What other elements need to be specified to assure the security of Company B's data?

(5 marks)

[PTO]

5 HUMAN BEHAVIOUR

a) Explain the difference between accessibility and usability.

(2 marks)

b) Explain how the Evaluate-Direct-Monitor process applies to the consideration of human behaviour affecting an information system.

(6 marks)

c) In response to the number of people who get out of speeding – and other motoring offenses – by claiming that they weren't at the wheel, the Home Office has commissioned a new system – Driver Identification After Motoring Offence using Numerous Databases (D.I.A.M.ON.D.) – to showcase joined up government and shared services. The objective is to positively identify the driver at the time of the offence beyond reasonable doubt. When a speeding car is caught by a forward-facing speed camera, the photograph of the driver's face is analysed biometrically. The result could be compared to the photographic record held by DVLA (cross referenced to the details of the registered owner). If no photographic driving license is held, or the suspect is not the registered owner, D.I.A.M.ON.D. could search for an identifying photographic record at (say) the Identity and Passport Service. If no photographic record at Identity and Passport Service, D.I.A.M.ON.D. may search for a photographic record of Foreign Nationals held by Home Office. When a matching photographic record is found, a report is sent to the local authority who manages the area where the speed camera is housed. Reports are reviewed to ascertain to whom the penalty notice should be sent.

Outline a plan that considers how the security of D.I.A.M.ON.D. may be affected by those who have to implement and use it and the measures to be taken to mitigate the resultant risks.

(4 marks)

Include an outline user acceptance test which includes the test of information security policies that are designed to mitigate the risk of human behaviour.

(4 marks)

Outline the human factors to be considered during the relevant activities across the system lifecycle:

- Concept Stage
- Development Stage
- Production Stage
- Retirement Stage

(4 marks)

END OF EXAMINATION