Two hours

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

IT Governance

Date: Tuesday 15th January 2013
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) Define the six elements of IT governance.  
      (12 marks)

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

   c) A hospital has the technical know-how and the budget to implement encryption technologies to protect the transmission of a patient’s records between the hospital and the patient’s General Practitioner.

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

   d) Describe – don’t just list - how can the opinions of the different stakeholders be collected and synthesised into a set of managed security requirements?  
      (3 marks)

2. **STRATEGY**

   a) What decisions must be made before taking reasonable accountability for entrusting critical information to public networks? Give examples of the risks to be considered.  
      (5 marks)

   b) List countermeasures that can protect data from the risks inherent in public networks. Make it clear which countermeasure applies to which risk.  
      (5 marks)

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

   d) The Manchester Broadcasting Corporation (MBC) is changing its business model. MBC had previously delivered programmes from the studios on physical media. Programmes were taken on tape or disc to the broadcasting facility in a delivery van. MBC wants to send programmes simultaneously to its own broadcasting facility and to those of other stations who have bought the rights to broadcast the programmes. They do not want any physical media to leave their premises. What are the implications of this change on the security of its intellectual property. Describe - in words and a labelled diagram – the architecture of a secure information system to protect MBC’s programmes during their distribution to the broadcasters: include the technology components, stakeholders, and interfaces where security is at risk.  
      (7 marks)
3. **ARCHITECTURE/STRATEGY AND ACQUISITION**

a) How can cloud computing improve the security of information? How can cloud computing threaten the security of information? (2 marks)

b) Explain how security may be managed through the supply chain. (2 marks)

c) RAMPARTS - **ReAl-time Mobile monitoring of Patient symptoms, Access to Records, Treatment, and Storage** – is an information system that processes and stores medical information about individuals and supports medical practitioners in their decision making and administration of treatment.

The basic requirements from RAMPARTS are:

1. Collect real-time data about a patient’s health from one or more medical devices carried by the patient.

2. Transmit that data to healthcare professionals who may:
   a. Administer medication or other treatment through one or more devices carried by the patient.
   b. Contact the patient with instructions. For example to take medicine or attend a clinic.

3. Create Electronic Health Records (an electronic version of the medical record of the care and treatment the patient receive; it’s kept up to date and looked after by the health care provider).

4. Update Personal Health Records (information about the patient’s health that the patient – or nominee - keeps up to date).

5. Aggregate data and make it available for medical research.
Technologies available include:

- Mobile medical devices
- Global positioning systems
- Applications
- Smartphones
- The mobile data network
- The Internet
- Short Message Service (SMS), e-Mail, Instant messaging (IM) etc.

Suggest a typical data set that is required to ensure the uninterrupted supply of information to medical devices carried by the patient. Divide this dataset into business impact levels to show the risks to it.

Design the information security architecture that will support the confidentiality, integrity, and availability of the information handled during the process of supplying the information or instructions for treatment. At what points will non-repudiation be important? Use a well-labelled block diagram. Build resilience into your design.

(16 marks)
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.

<table>
<thead>
<tr>
<th>Level</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Optimizing</td>
</tr>
<tr>
<td>1</td>
<td>Quantitatively Managed</td>
</tr>
<tr>
<td>2</td>
<td>Incomplete</td>
</tr>
<tr>
<td>3</td>
<td>Managed</td>
</tr>
<tr>
<td>4</td>
<td>Performed</td>
</tr>
<tr>
<td>5</td>
<td>Defined</td>
</tr>
</tbody>
</table>

(5 marks)

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

(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)
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) The Barsoomian Arthritis Research Foundation coordinates multinational activities to do with the treatment of arthritis and research into new and improvement treatments. Its activities include coordinating drugs trials for different pharmaceutical corporations, surveys into the epidemiology of the condition, and advice for arthritis sufferers. Its systems vary from data collection to self-help websites. The Foundation employs 150 people and relies on the good will of volunteers to collect funds and disseminate its publications. It may be coordinating the activities of 50 local charities as well as its own activities at any one time. Registered arthritis sufferers are given free access to advisory materials and counsellors who can help them cope with what is often a debilitating condition.

   Identify three types of information system that the Foundation will benefit from and select the one with the highest risk to the Foundation’s reputation if it fails to deliver its expected benefits. Describe the human factors that must be considered through

   
   - Concept Stage
   - Development Stage
   - Production Stage
   - Utilization Stage
   - Support Stage
   - Retirement Stage

   How should these human factors be managed to keep the risk of human errors or sabotage to a minimum?

      (12 marks)

---

**END OF EXAMINATION**