

Two hours

Please use a ruler for diagrams and tables

**UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE**

IT Governance

Date: Tuesday 17th January 2017

Time: 09:45 - 11:45

Please answer any THREE Questions from the FOUR Questions provided

**Do NOT use one-word answers or use lists without an explanation of each element in the list.
No marks will be awarded for reproducing answers to similar questions from previous years.**

This is a CLOSED book examination

The use of electronic calculators is NOT permitted

[PTO]

1. RESPONSIBILITY AND ACQUISITION

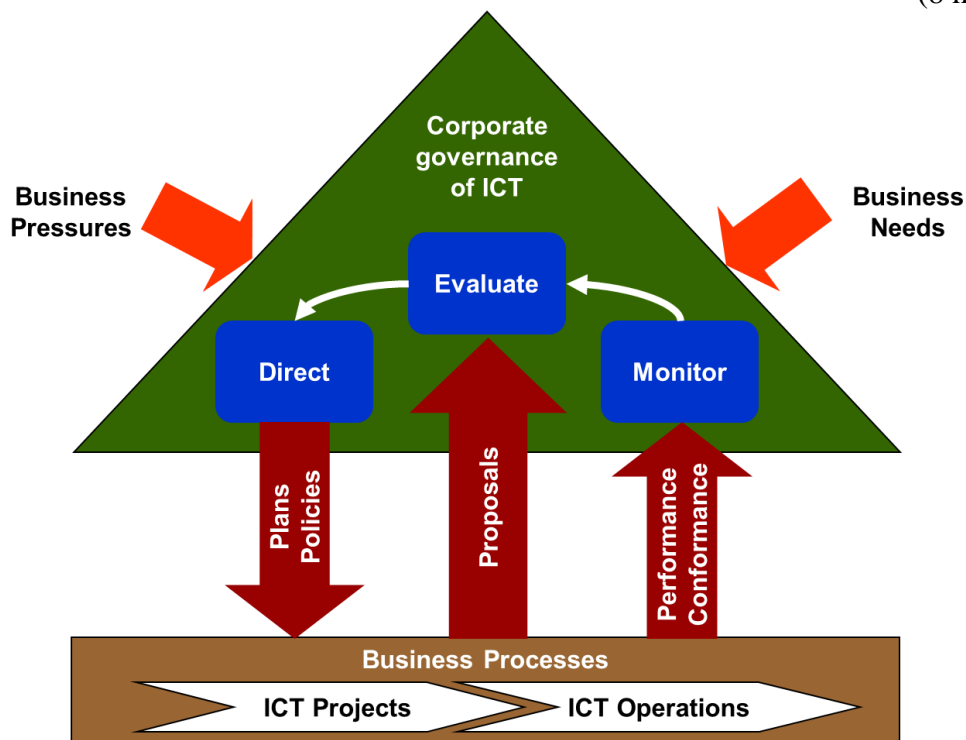
- a) Explain – in your own words – the six elements of IT governance. (6 marks)
- b) According to the Soft Systems Methodology, what are the three types of people associated with the governance of an information system. How can they be mapped to those involved in the acquisition and deployment of an active system? (6 marks)
- c) The Callous and Bonzo Confectionery Company has a process control system that is used for making its famous, chocolate-coated liquorice toffees. The marketing department has determined that the company will sell more sweets if it puts a thicker layer of chocolate on them. However, when the process control system was procured in 1962, it was not designed to allow any variation in the recipe used on the production line.

Explain how the standard process for IT Governance – as laid down by ISO/IEC 38500 – should be applied to upgrade the system.

Who is involved with the respective parts of the process? Be specific to the likely stakeholders in the case study.

Use a well-labelled diagram with supporting commentary.

(8 marks)



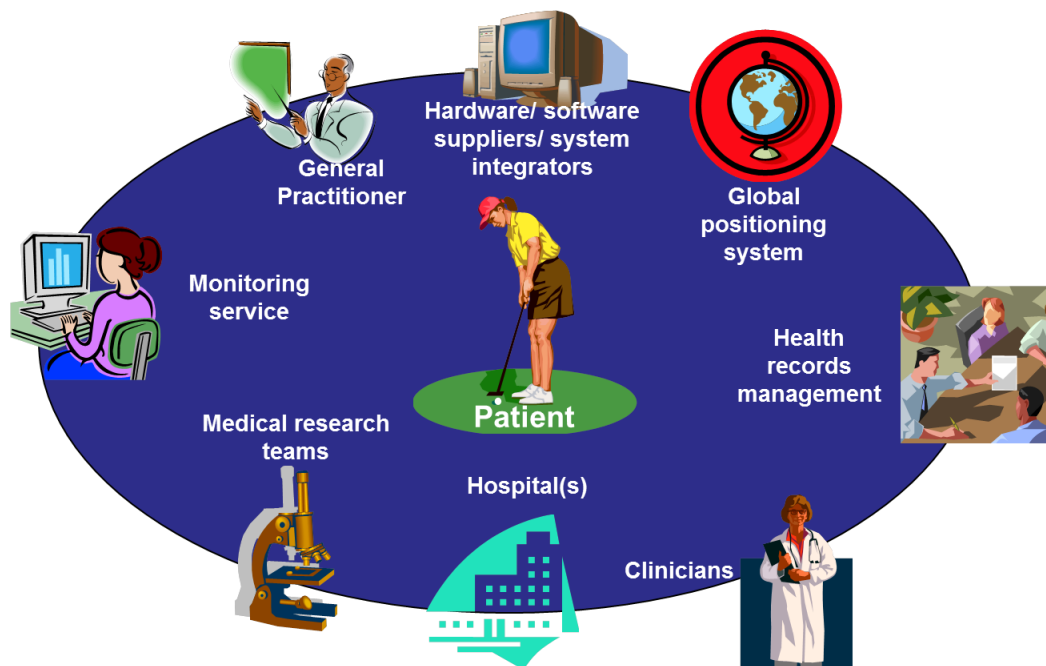
ISO/IEC 38500 Model for Corporate Governance of IT

2. ARCHITECTURE/STRATEGY

a) Explain the role of the reference architecture in IT Governance.

(2 marks)

b) RAMPARTS - **R**eAl-time **M**obile monitoring of **P**atient symptoms, **A**ccess to **R**ecords, **T**reatment, and **S**torage – 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 receives; 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.

[PTO]

Technologies available include:

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

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. Consider, in particular, the importance of protecting patient-identifiable data. Use a business impact table to present your solution.

(6 marks)

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.

(12 marks)

3. **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

(6 marks)

- b) Explain two different classes – not example - of metric. How do they contrast?

(2 marks)

- c) Design (in outline) a real-time tool for IT governance, using leading and lagging metrics. What will the tool show? What decisions could the tool support? How might the tool be used? Use tables and diagrams appropriately.

(12 marks)

[PTO]

4. HUMAN BEHAVIOUR

- a) Explain the difference between accessibility and usability. (2 marks)
- b) Explain how a system must account for human behaviour in its design throughout its life cycle from conception to decommissioning. What is the appropriate role of training and education? (3 marks)
- c) Explain how the responsibilities in the Evaluate-Direct-Monitor process apply to the consideration of human behaviour affecting an information system. (3 marks)
- d) Redfriars school has 300 pupils and 50 staff including administration, building maintenance, a school nurse, and (of course) teachers. Some of the teachers also provide careers advice and social counselling to the pupils. The school is managed by a panel comprising 3 governors (including a parent governor), a bursar (managing the accounts) and the headmaster.

Information needs to be kept on each pupil including attendance records, special needs including dietary requirements, parent or guardian contact details, marks from school work and examinations, and membership of extra-curricular clubs, behavioural and disciplinary records, and financial records about the payment of school dinners and school trips.

Over the years, the information system has been built up piecemeal and comprises half a dozen PCs networked across the school with a central server in the head teacher's office. A benefactor from their local computer dealer, the Universe of IT Emporium (UNITE), has offered to replace – at UNITE's expense – the current kit with a new school server and wireless router, wireless network laptops for each teacher, workstations for each pupil and administrative staff, and database programming expertise to create a new school management information system. Pupils will be allowed to bring their own devices for use on the school network.

- i) Make a list of use and misuse cases that must be considered to ensure that the upgraded system will deploy good security practices which protect the information about the stakeholders in the system and enable the effective running of the school. (3 marks)
- ii) Use the list of use/misuse cases to carry out a high-level business impact assessment (BIA) for the upgraded system. Show this in a business impact table. (4 marks)
- iii) Design an integrated set of countermeasures to reduce the risks arising from human factors identified in the BIA. Make it clear – by using a table – which countermeasure should be applied to mitigate the respective risks. (5 marks)

END OF EXAMINATION