Two hours

Please use a ruler for diagrams and tables

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

IT Governance

Date: Monday 22nd January 2018

Time: 14:00 - 16:00

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

(a) Why is good governance a prerequisite for security?

(3 Marks)

(b) 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.

Explain the dynamics of decision rights and escalation paths between people, between people and machines, and between machines?

(5 Marks)

(c) Who needs to be involved to make this bank’s security technology an enabler not a hindrance?

How can the opinions of the different stakeholders be collected and synthesised into a set of managed requirements? Consider functional and non-functional matters. Comment on the strengths and weaknesses of different methods.

(12 Marks)

2. CONFORMANCE AND PERFORMANCE

(a) Explain the structure of the IT governance maturity model.

(3 Marks)

(b) What are leading metrics? What are lagging metrics? And what is the risk of relying on one type?

(5 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.

Create a balanced scorecard of performance measures that will show that the dataset is adequately monitored for levels of confidentiality, integrity, and availability, that will meet the business objectives.

(12 Marks)

3. HUMAN BEHAVIOUR

(a) Why is relying on user education and training a high risk approach to information security?

(3 Marks)

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

(5 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.

Consider use and misuse cases to 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.

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

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

What non-functional attributes need to be designed in - and give examples of how they can be measured or tested for - to mitigate the risk of inappropriate (human) behaviour?

(12 Marks)

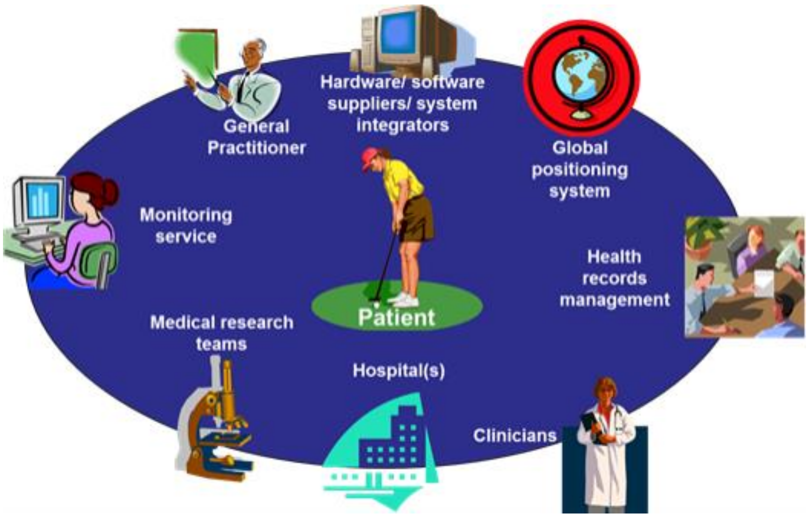
4. GENERAL

(a) What are the six principles of IT Governance? Explain each–don't just list them

(3 Marks)

(b) How do the principles of IT Governance work with the process of IT Governance?

(5 Marks)


General Practitioner
Hardware/ software suppliers/ system integrators
Global positioning system
Monitoring service
Health records management
Patient
Medical research teams
Hospital(s)
Clinicians

(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:

- Collect real-time data about a patient's health from one or more medical devices carried by the patient.
- Transmit that data to healthcare professionals who may:
  - Administer medication or other treatment through one or more devices carried by the patient.
  - Contact the patient with instructions, for example, to take medicine or attend a clinic.
  - 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).
  - Update Personal Health Records (information about the patient's health that the patient - or nominee - keeps up to date).
  - Aggregate data and make it available for medical research.

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)

END OF EXAMINATION