No calculator permitted

UNIVERSITY OF BIRMINGHAM

School of Computer Science

MSc Cyber Security

06 28213

Secure System Management

Summer May/June Examinations 2017

Time allowed: 1 hour 30 minutes

[Answer ALL Questions]

1. Versions of ISO 27001 vary in the options they give for managing continuous improvement, but all permit a "Plan Do Check Act" cycle. Describe how this cycle's four stages can be used in the operation of an Information Security Management System (ISMS). [25%]

2. An ISMS has as a key component a risk treatment plan, which considers risks and applies controls.

   (a) Explain with examples what is meant by a control (i) reducing, (ii) mitigating and (iii) transferring a risk. [9%]

   (b) A risk treatment plan might instead accept a risk. Explain why this decision might be taken, and give an example of a situation when it may be a good response to a risk. [6%]

   (c) Once a risk treatment plan has been produced, a document will be prepared summarising the level of risk left untreated. Name this document, and explain its purpose both within an ISMS and more widely for management of the enterprise. [10%]

3. An important element of an ISMS is the collection of metrics.

   (a) Suggest a metric which might be collected to track the performance of a process which adds and deletes users from the system, and explain why this is useful when analysing the operation of an ISMS. [5%]

   (b) Metrics which directly measure serious events have the problem that in a given year there will most likely be zero, and at most one, such event. How does the concept of a "near miss" give more information about the likelihood of the event occurring? [10%]

   (c) Metrics are collected at various points in the ISMS. What mechanisms can be used to check that this is done correctly and honestly? [5%]

   (d) Why is it important that both internal and external audit are carried out on an ISMS? [5%]

4. A threat actor can be said to have motivation and capability.

   (a) Give an example of a threat actor who has a high motivation but a low capability. What sort of attacks might such an attacker be able to conduct? What controls might be effective against the risk they present? [8%]

   (b) Give an example of a threat actor who has a low motivation but a high capability. What might you write in a risk treatment plan to address this threat actor? [8%]

   (c) What will be the effect on a risk treatment plan if motivation is ignored in a risk assessment? [9%]

Do not complete the attendance slip, fill in the front of the answer book or turn over the question paper until you are told to do so

Important Reminders

- Coats/outwear should be placed in the designated area.
- Unauthorised materials (e.g. notes or tippex) must be placed in the designated area.
- Check that you do not have any unauthorised materials with you (e.g. in your pockets, pencil case).
- Mobile phones and smart watches **must** be switched off and placed in the designated area or under your desk. They must not be left on your person or in your pockets.
- You are not permitted to use a mobile phone as a clock. If you have difficulty seeing a clock, please alert an Invigilator.
- You are not permitted to have writing on your hand, arm or other body part.
- Check that you do not have writing on your hand, arm or other body part – if you do, you must inform an Invigilator immediately
- Alert an Invigilator immediately if you find any unauthorised item upon you during the examination.

Any students found with non-permitted items upon their person during the examination, or who fail to comply with Examination rules may be subject to Student Conduct procedures.