- No calculator permitted in this examination

THE UNIVERSITY OF BIRMINGHAM

THIS PAGE TO BE REPLACED BY OFFICE

06 28213

Secure System Management

June 2016 1 hour 30 minutes

[Answer ALL questions]

1. An enterprise responds to *risks* to its security with a *risk treatment plan* which amongst other things applies *controls*.

   (a) A risk may be *reduced*, *mitigated*, *transferred* or *accepted*. Briefly describe the difference between these responses, and for each give an example of a risk for which it is the most appropriate response. **[12%]**.

   (b) A risk treatment plan arises out of a *risk assessment* which evaluates *threat actors*. In the context of risk assessments, distinguish between the *motivation* and *capability* of a threat actor. Give an example of a motivation and an example of a capability. **[6%]**

   (c) Give an example of a threat actor whose motivation presents a low risk but whose capability is formidable, and an example of a threat actor whose motivation is substantial but who does not present a serious risk to a well-run enterprise. Justify your examples. **[10%]**

2. A business decides to reduce the risk of unauthorised access to its systems by installing a VPN and removing all other means of access to internal systems. Users will no longer be able to access corporate systems from computers they own and control. Under the new policy, only company-controlled laptops will be able to access corporate systems, using two-factor authentication, and all such access will require approval by a senior manager.

   (a) Describe two risks that this policy either *mitigates* or *reduces*. **[8%]**

   (b) Describe the impact of this change on the ability of the company to audit and control its perimeter security. Pay particular attention to issues of cost and complexity. **[10%]**

   (c) Users do not always follow rules and procedures, and changes are sometimes resisted. What negative consequences might arise from this change? What could be done to reduce their impact? **[10%]**

3. ISO 27001 mandates both *internal audit* and *external audit* to check compliance with *policies* and *procedures*.

   (a) Briefly distinguish between internal and external audit. **[6%]**

   (b) Describe the rôle of *quality records* in audit. **[6%]**

   (c) Distinguish between a policy and a procedure. Give an example of what might be found in each of them. **[6%]**

   (d) ISO 27001 requires that a company publish the *scope* and *statement of applicability* of their certification. What is in each of these two documents? **[8%]**

   (e) Describe the purpose of a *residual risk statement*. Why is it necessary that this be signed by senior management in an enterprise? **[6%]**

4. Security management policies require the collection of *measures of effectiveness*, otherwise known as *metrics*.

   (a) Describe two metrics a company might keep to measure the effectiveness of its user account creation and deletion process. **[6%]**

   (b) An audit report shows that non-compliances in the area of account deletion are increasing. What might you investigate, and what measures might you institute, in response to this? **[6%]**