Solutions to Student Self Assessment Questions

Chapter 7

Systems work: basic ideas 1

Questions

7.1 Explain the importance of internal control within organizations. What are the main elements and what is the auditor's interest in them?

7.2 Integrity and ethical values are important factors in ensuring that internal control, including the control environment is effective in reducing risk and in helping management to achieve objectives. Do you think that these are just meaningless words or are they really important in the business context? Why do you think that auditors look for integrity and ethical values in management and throughout the organization?

7.3 You have recently become auditor of a small trading entity whose system is based on a series of networked microcomputers, using bought-in software for basic accounting functions. During the initial meeting with management, the managing director told you that he is really scared of all 'this computer stuff', particularly as there is no one in the entity who has any specialized knowledge of computers. How would you advise him? What do you think might be the key risks in such a entity?

Solutions

7.1 Internal control is defined in Paragraph 4 (c) of ISA 315:

The process designed, implemented and maintained by those charged with governance, management and other personnel to provide reasonable assurance about the achievement of an entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations. The term "controls" refers to any aspects of one or more of the components of internal control.

Note its aims:
(a) To ensure within reason that financial reports are valid and reliable
(b) To ensure within reason, that operations are effective and efficient
(c) To ensure within reason that applicable laws and regulations are adhered to
(d) To address identified business risks that may threaten the objectives in (a) to (c) above.

The main elements (or components) of internal control are:
(a) The control environment.
(b) The entity's risk assessment process.
(c) The information system, including the related business processes, relevant to financial reporting, and communication.
(d) Control activities.
(e) Monitoring of controls.

The reason that the auditor is interested in the effectiveness of internal control and its components is that good control systems reduce audit risk by mitigating the impact of inherent risk. The auditor's main interest, of course, is in determining that the financial statements give a true and fair view, and the existence of strong internal control within the organization will increase the likelihood that financial reporting is valid and reliable. If control risk is low the auditor will be able to reduce the amount of detailed substantive testing.

ISBN 978-1-4080-3049-3

7.2 We saw in the text that the control environment can only be effective if integrity and ethical values permeate the organisation. However, they CAN be just meaningless words unless management makes sure that staff know what integrity means in the context of the organisation. For instance, management of an electrical retailer would effectively be saying to customers that goods purchased were safe to use. This would mean that statements about safety would have to be properly backed up by a proper testing regime. If not, the company would expect to suffer loss of reputation and to incur damages as the result of court cases. An example like this can show us that integrity and ethical values have a practical significance and are not just meaningless words.

As far as auditors are concerned, they have to decide if they can rely on company systems in achieving their own objectives, the main one of which is to give an opinion on the truth and fairness of the financial statement. Management is responsible for putting in systems and creating a control environment that will ensure that all of their objectives will within reason be met, including preparing financial statements that truly and fairly represent the results of the organisation and its state of affairs. If management possesses integrity and ensures that company staff are aware of the ethical values needed in the context of the company, the auditor will be more confident that the control environment and associated detail controls can be relied on. In this connection, there have been a number of well-publicised case of whistle-blowing by people internal to organisations, who have objected to the way that the organisations behave. Very often these objections are legitimate and organisations should have a stated policy in respect of whistle-blowing, including a system that enables employees to discuss their misgivings to independent people within the organisation.

7.3 You might have preferred not to start from here, but rather to have been involved when the decisions were made to install the computer system. The key risks would be as follows:

a) Physical risks affecting the microcomputers, the network server and the people operating systems. You might suggest to the managing director that he should ensure that physical equipment should only be used by authorised people and be kept secure particularly outside working hours. It might be useful to employ someone with basic computer skills to help staff when problems arise and to make sure that the server is working properly when needed. It might also be desirable to shut down the server outwith normal working hours. This person might usefully draw up a code of conduct for computer users, including a restriction in the time that people sit at the keyboard.

b) Risk that the system has not been developed properly in the first place. You should ask the managing director to see the documentation prepared at the time the system was developed, including any feasibility studies, documentation concerning the desired characteristics of the systems, and testing that was carried out, and by whom, prior to putting the system into use. You would be particularly interested in discovering if the bought-in software performs in the way expected, for instance, whether appropriate information/audit trails are recorded. Is double entry properly carried through in all cases? You should also ask what kind of training staff received at the time the system was introduced and what kind of ongoing training is provided. For instance, was staff informed of the need to respond to error messages, to keep passwords private, and to report bugs in the system.

c) Risks of loss of programs and data. The managing director might be particularly concerned about loss of (say) trade receivables, trade payables and inventory records, and information used to manage the business. We are not told much about the system but we would recommend simple security measures, such as

keeping back up copies of programs and data outside the operating areas, supported by the use of grandfather, father, son and dumping systems as appropriate. You should advise the managing director to establish degrees of access to data if this has not been done already, supported by the use of appropriate passwords. You might also suggest that one person keep master copies of programs and of back-up copies of data in a computer library, together with a booking in/out system.

d) Risk that the company does not observe appropriate organisational controls. For instance, does the company have a system for allocating responsibility? Are duties appropriately segregated? You might reassure the managing director that in a small company where there is little computing knowledge among staff and where systems analysts and programmers are not employed there is a lower risk that people will interfere with the proper operation of programs.

ISBN 978-1-4080-3049-3