

# **AUDIT & ASSURANCE**

**December 2004  
Diploma stage**

## **MARKING SCHEME**



(Copyright)

**NOTE: In all cases marks will be awarded to appropriate answers even if not directly covered by the marking scheme**

**Question 1**

(a) Planning analytical procedures for leisure services:  
(NB. Marking scheme is indicative only. Credit will be given for other appropriate procedures)

- Leisure centre contract – Compare budget versus outturn. Most variable activity is responsibility of the contractor so any significant deviations from the agreed fee should be investigated.
- Playing fields – compare total income levels over last two years and budgeted income for this year. Look for significant variations.
- Identify seasonal variations in income (eg football in winter, cricket/tennis in summer) and compare actual income to profile to identify patterns which do not conform to what you are expecting.
- Calculate average income per type of field and compare over last two years. Look for significant variations in average income.
- Obtain list of users and compare to lists of invoices raised to identify potential omissions.
- Calculate average costs of staff/supplies/equipment hire etc. per hectare or playing field to identify significant variations.
- In all cases compare previous year's actual costs to this year's budget to highlight any predicted variations which will explain differences in outturn figures and discuss with leisure services management.

*Up to 2 marks per procedure well explained up to a maximum of 8*

(b) Differences between audit risk and business risk:

Dear Mr Leary

Thank you for your e-mail. I hope I can clarify the situation with regard to the differences between your business risk assessment and our audit risk assessment.

To a large extent what you say is true – the sorts of risks that you have to deal with in your area or operations are the same as the ones we are interested in from an audit point of view. However, there are differences which relate to the way in which we carry out our audit work.

Business risk is the risk that an organisation will fail to meet its objectives in some way. It is usually analysed into three components ie those arising from the financial activities of the organisation, the operation of the business or the risk of non-compliance with laws and regulations.

Auditors can make use of management's business risk assessment in determining the factors which make certain aspects of the business more risky than others.

Auditors must also assess audit risk, which is the risk that auditors will fail to spot material errors or significant weaknesses in the system. We analyse audit

risk into three components as well: ie inherent risk, control risk and detection risk.

These are the risks that errors or mistakes may happen in the first place owing to the environment in which the organisation operates, the risks that management's internal controls will fail to prevent or detect those errors that do occur and the risk that audit procedures will fail to detect major errors or weaknesses.

Business risk is assessed in order to help managers decide how best to manage those risks including designing appropriate internal controls and keep them within acceptable limits. Auditors use their assessment of risk to decide on the appropriate level and type of audit work to carry out in order to reduce audit risk to an acceptable level.

We appreciate your co-operation in this review and I hope if you have any further questions you will not hesitate to get in touch.

*Up to 3 marks for definition of components of business risk;  
Up to 3 marks for definition of components of audit risk;  
Up to 2 marks for other relevant points  
1 mark for memo format, tone etc.  
Total for part (b) - 9*

**(c)** Memo to IA manager on systems development approaches:

From: Senior internal auditor  
To: Audit Manager – HIA  
Subject: Audit involvement in IT systems development  
Date: DD/MM/YY

You asked me for an outline of the ways in which we might approach any involvement in the development of the new computerised electoral register.

Our two options are:

- To wait until the system is developed and then conduct a review of how the process was managed; or
- To be involved from the outset and take a pro-active stance with regard to the development of the new system.

The advantages of the two approaches are:

**Review the system after it is developed**

- Less costly in terms of audit input therefore less cost to organisation.
- Reduced demand on scarce computer audit skills.
- Less IA commitment in terms of time over next two years.
- Less potential embarrassment to IA if the project goes badly.
- Avoids potential risk to audit objectivity and independence.

**Involvement in development process**

- Higher profile/status for IA function with management.
- Opportunity to have appropriate controls built in from the start makes audit of system easier.
- Less costly or disruptive to organisation to make changes to the system at the outset rather than after it has been implemented.
- IA is more familiar with the system when reviewing operations.
- Independent oversight in the development process gives validation to management.

I hope this helps. Please call me if there is anything else you need to know.

*1 mark for each option identified; ½ mark for each advantage  
up to a maximum of 7*

*1 mark for memo format and style*

*Total for part (c) - 8*

**(d) Application controls:**

The purpose of application controls is to ensure the completeness, accuracy, security and effectiveness of processing. They may be provided either by programming within the application system or by manual controls exercised by users or the IT department.

Application controls are specific to a particular system and cover such things as:

- input;
- processing;
- storage; and
- output

of data.

Examples of possible application controls in the electoral register:

- Input – Data validation check. Computer to reject duplicate entries of the same name at the same address.
- Processing – Changes to standing data, eg date of birth, must be authorised by section supervisor.
- Storage – Backup files to be securely stored to prevent unauthorised access.
- Output – Register of authorised recipients of electoral rolls to be maintained and periodically checked for accuracy by management.

*2 marks for definition of application controls*

*1 mark per example up to a maximum of 4*

*Total for part (d) - 6*

**(e)** Internal audit communication with audit committee:

- Quarterly written report by HIA to Committee on progress against plan.
- Annual summary report to committee on activity during year.
- Annual report to include key performance indicators eg cost per audit; savings identified; % recommendations accepted; % reports issued on time.
- Attendance of HIA at all committee meetings to answer questions/give advice to members.
- All IA reports to be presented to/cleared with committee before being issued.
- HIA to attend and give verbal report to committee on all reports issued.
- HIA to report on progress in implementing agreed audit reports.

*1 mark per point made up to a maximum of 5*

**(f)** Local government standards for Internal Audit:

- Relevant APB Statements of Auditing Standards (eg Audit Sampling; Working Papers).
- CIPFA Statement of Professional Practice on Auditing (1995).
- APB Auditing Guideline 308 – Guidance for internal auditors.
- CIPFA Code of Practice for Internal Audit in Local Government in the United Kingdom (2003).
- Relevant IIA standards.

*1 mark per point up to a maximum of 4*

**(40)**

**Question 2****(a)** Audit guidance issued by the APB.

**Practice Notes.** These assist auditors in applying Auditing Standards of general application to particular circumstances and industries. Examples would include PN 10 on the application of SASs to audit of public sector entities; or PN 12 on the audit of charities.

**Bulletins.** These provide auditors with timely guidance on new or emerging issues. These are usually withdrawn when the issue is no longer relevant or included in new or revised SASs if they are of continuing impact.

Both bulletins and practice notes are of persuasive rather than prescriptive authority. They are indicative of good practice and have equivalent status to the explanatory material in the standards.

*Up to 2 marks for each point fully explained to a maximum of 5*

**(b)** Qualified audit opinions under SAS 600

- The matter must be material if auditors are to consider qualifying their opinion. Non-material errors or omissions will not result in qualification.
- If the matter can be corrected and audited body is prepared to alter the accounts then no qualification is necessary.
- Auditors may qualify on the grounds of disagreement with figures or statements in the accounts eg failure to comply with FRS or other reporting requirement.
- Or they may qualify owing to uncertainty over their opinion ie lack of evidence to support the financial statement assertions.
- If disagreement is material, auditors will qualify their opinion and seek to quantify the effect of the disagreement on the financial statements.
- Form of opinion would be “Except for ... the financial statements give a true and fair view.”
- If lack of evidence is on a material matter then auditors qualify on the basis of a scope limitation.
- Form of opinion is “Except for any adjustments which might have been necessary if we had been able to obtain all the evidence ... the financial statements give a true and fair view.”
- Disagreement or uncertainty may be so material or pervasive as to make the statements seriously misleading or make it impossible for the auditors to form an opinion on them.
- Fundamental disagreement results in an adverse opinion “In my opinion these financial statements do not give a true and fair view.”
- Fundamental uncertainty results in a disclaimer “I am unable to form an opinion on these financial statements.”

*1 mark each point fully explained, to a max of 8*

**(c) Opinions required:**

- |  |   |
|--|---|
| (i) Material disagreement with the legality of the amounts in the account – qualified opinion on grounds of disagreement.  | 1 |
| (ii) Lack of evidence on a material part of the amounts contained in the statements – qualified opinion on the grounds of scope limitation.  | 1 |
| (iii) Fundamental uncertainty as to the basis on which the accounts have been prepared. Disclaimer opinion, since the auditors are unable to express an opinion.   | 1 |
| (iv) Disagreement on accounting treatment where the effects are so pervasive as to destroy the truth and fairness of the accounts (profits, fixed assets, debtors, provisions and long term contracts are all misstated). Adverse opinion. | 2 |
| (v) Fundamental inherent uncertainty since the matters relate to the resolution of future events with implications for going concern.  |   |
| • If the matter is adequately disclosed in the accounts then no qualification is needed but the auditors will include an explanatory paragraph in their report.  | 1 |
| • If the matter is NOT adequately disclosed – Adverse opinion (omission of something fundamental to obtaining a true and fair view).   | 1 |

*Total for part (c) – 7*

**(20)**

**Question 3**

- (a) Internal Auditors' responsibility with regard to prevention and detection of fraud:
- determined to a large extent by reference to IA's objectives, as determined and agreed by management.
  - primary responsibility for the prevention and detection of fraud rests with management.
  - internal audit should act to support them in this role.
  - Institute of Internal Auditors states that: internal auditors should have sufficient knowledge to identify the indicators of fraud.
  - IA not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.
  - IA plan their work and design their testing with regard to the possibility that fraud may occur.
  - control weaknesses which might allow fraud to occur should be highlighted to management.
  - auditors may wish to carry out some testing to see if weaknesses have actually been exploited.
  - where evidence or reasonable suspicions of fraud arise, these should be reported to the appropriate level of management.

*1 mark per point up to a maximum of 9*

- (b) Memo to HIA:

**INTERNAL MEMORANDUM**

From: Head of anti-fraud unit  
To: Head of Internal Audit  
Date: DD/MM/YY  
Subject: Anti-fraud strategy at ABC public sector organisation

**Introduction**

ABC has had a history of petty fraud for a number of years and there seems to be a lack of commitment on the part of management to improving the situation. In this memo I will seek to explain:

- why management need to take the situation more seriously; and
- what the anti-fraud unit can do to address the situation.

**Why management need to take the situation seriously**

The first point to make is that whilst the scale of fraud is relatively small at present, this could very easily and quickly get worse. Reported fraud is very often a lot less than the actual level, so the situation could already be more serious than management believe it to be.

The fact that much of this fraud is committed by staff within the organisation makes this all the more likely, since it is easier for internal frauds to be both perpetrated and concealed when fraudsters have access to the systems and records of the organisation.

The fact that frauds even extend to management grades is particularly worrying, since the message this sends to the rest of the workforce is that fraud is acceptable.

There continues to be great focus on the governance arrangements in public bodies. The high standards of ethics and probity demanded of individuals working in the public sector mean that the current situation represents a severe risk to the reputation of both individuals and the organisation.

By allowing the situation to continue there is also a threat to the normal operation of the organisation's business since the suppression of control procedures associated with internal frauds may allow more genuine errors to get through the system, affecting the reliability of both financial and management information.

*Up to 1 mark for each point made to a maximum of 5*

### **Action to address the situation**

By setting up the anti-fraud unit the audit committee have indicated their commitment to addressing this issue. We should therefore build on this by meeting with the committee to seek their views and obtain their support for the establishment of a formal anti-fraud strategy.

The strategy should be promulgated by the committee to reinforce the message that it is management's responsibility to prevent and detect fraud and the existence of the unit in no way reduces that primary responsibility.

The strategy should contain a clear statement that fraudulent activity is not acceptable and that there will in future be a strict policy of prosecution and disciplinary action against all staff found to have defrauded the organisation.

Following that we need to carry out a series of top-down discussions with heads of department to obtain their support and commitment to what we are doing. It is imperative that we persuade management to take the matter seriously. If we cannot then introducing tighter control mechanisms will not work because staff will not implement them.

One way of doing this is to get management more involved in the control mechanisms of the problem areas such as stores or expense claims. This will draw their attention to the problems in the area and further reinforce management's commitment to eliminating the problem.

The single biggest source of information on actual and potential fraud is the staff themselves. We should therefore set up a confidential whistle-blowing hot line to allow staff to report actual or suspected cases of fraud amongst their colleagues directly to the anti-fraud unit.

*Up to 1 mark for each point made to a maximum of 5  
1 mark for appropriate memo format, introduction etc.*

**(20)**

**Question 4**

(a) Three main components of an effective internal audit function:

- Compliance with relevant standards.
- Appropriate framework for operation of internal audit.
- Independence in terms of objectivity and status.

*1 mark for each point to a maximum of 3*

(b) Factors contributing to the effectiveness of internal audit:

**Positive**

- High level of professional qualification amongst audit staff encourages high quality work and independent objective stance.
- Training programme demonstrates commitment to maintaining skills.
- Terms of reference show primary responsibility to audit committee.
- Automatic right to go to Chief Executive or Committee allows for independent reporting.
- Scope of internal audit activity not subject to influence by managers of services.
- Access to documents and staff enshrined in terms of reference safeguards scope of audit.
- Physical location may help maintain independence and objectivity.

**Negative**

- In-house staff may form personal or close working arrangements with client departments leading to loss of objectivity. (Also familiarity of previous head with directors may have re-enforced this.)
- Loss of well-known contact with departments may hamper co-operation in carrying out reviews.
- Secondment of staff from IT section may compromise objectivity and independence if asked to audit systems they previously worked on.
- Grade of HIA relative to other heads of service indicates a possible low perception of status of IA in practice.
- Budget holder is finance director which may cause a reluctance to criticise them in audit reports.
- Physical location may indicate low status – IA forgotten about when new building was planned.
- Out of date manual and programmes likely to mean poor quality audit and thus reflect adversely on perception of audit as a modern professional service.

*1 mark for each point to a maximum of 12*

(c) **Immediate** steps to address negative factors:

- Detail one of the senior staff to update the manual to ensure it complies with current standards and best practice.
- Get one of the junior staff to identify programmes which need updating and whether this needs senior auditor input.
- Review work plan of IT auditor to ensure they are not reviewing systems for which they had operational responsibility.
- Seek re-grading of HIA post to level commensurate with status and responsibilities.
- Set up meeting with heads of departments to introduce yourself to them and discuss IA work plans in their area.

*1 mark for each point to a maximum of 5  
(½ mark for longer term actions eg re location)*

**(20)**

**Question 5**

- (a) Types of controls and risks for which they are appropriate:  
(NB risks are indicative only and students will be given credit for other relevant risks.)

Type of control	Risk
Segregation of duties	Risk of one person having complete responsibility for all stages of a process
Organisational	Risk of delegating responsibility to an inappropriate level
Authorisation and approval	Risk of unauthorised and invalid data entering a system
Physical	Risk of loss or damage to the tangible assets of an organisation
Supervision	Risk of failure by staff to comply with proper procedures
Personnel	Risk of employing or appointing staff without the relevant skills or experience to carry out their assigned duties
Arithmetic and accounting	Risk of accounting errors such as mis-coding or omission
Management	Risk of cumulative errors or unusual transaction slipping through other controls

*½ mark per type of control and ½ mark per risk to a maximum of 8*

- (b) Risks and Controls:

- (i) Risk is loss of sensitive information if laptop or disks are lost or stolen. Prevent by encryption of data.
- (ii) Risk that new staff will not be up to date on H&S legislation. Prevent by checking of qualifications and experience of applicants for posts.
- (iii) Risk of staff not being removed from the payroll when they cease working. Prevent by supervisors submitting list of all casual staff employed each week and checking to payroll system.
- (iv) Risk of new system not being able to support business needs of the organisation. Prevent by ensuring full feasibility study carried out and specification drawn up by project team after consultation with users.

*Up to 2 marks per point – 1 for risk and 1 for control – to a maximum of 8*

(c) Other methods of managing risk:

- The decision on which strategy to adopt should be based on an assessment of the likelihood of the risk materialising and the potential impact (both financial and operational).
- Accept – if the likelihood is very low and the impact is minor then it may be best just to accept the risk.
- Insure – if the likelihood is low but the potential impact very high then insuring or otherwise transferring the risk may be the best method of dealing with it.
- Avoid – if the risk cannot be controlled or transferred and the consequences are too serious to accept, an organisation may choose to stop doing whatever it is that is exposing them to the risk.

*1 mark per point to a maximum of 4*

**(20)**