CIPFA

AUDIT AND ASSURANCE

Diploma stage examination

8 June 2007

MARKING SCHEME

AT THE HEART OF YOUR CAREER

Question 1

(a) Provide a definition of internal audit

Internal audit is an appraisal activity established within an organisation. Internal audit is normally assigned specific responsibility by management for reviewing controls, monitoring their operation and recommending improvements where necessary.
Internal audit will therefore objectively examine and evaluate the internal control systems as a service to the organisation.

The scope of internal audit should not be restricted, in order to maintain objectivity and independence; for example by:

- Having unrestricted access to records, assets and personnel.
- Having the right to report to all levels of the organisation.
- Determining their own priorities and plans, in consultation with management.
- Having personnel with an objective attitude of mind.
- Having personnel who have no non-audit work.

1 mark for definition of internal audit, 3 marks for other points made up to maximum of (4)

(b) Advantages of outsourced provision of internal audit

Advantages may include:

- Clear independence from the management of the organisation.
- No staff administration and training requirements falling on the organisation.
- Cross fertilization of ideas and best practice from other sources and sectors.
- Flexible resource availability.
- Full access to technical expertise and ancillary services.
- A flexible contract, you only pay for what is delivered.

1 mark per relevant point made up to maximum of (4)

(c) (i) Audit planning process

The purpose of planning for audit is to:

- Determine priorities and establish the most cost-effective way of achieving objectives.
- Assist in the direction and control of audit work.
- Estimate resources required to meet audit needs.
- Ensure that attention is devoted to critical aspects of audit work.
- Ensure that work is complete in accordance with pre-determined targets.
- Ensure that audit work generates sufficient evidence to support the audit opinion.

1 mark per relevant point made up to maximum of 3

(ii) Understanding the client

Understanding the business:

- The regulatory environment in which it operates.
- The organisation's own policies and objectives.
- The characteristics of the organisation (size, complexity, etc).
- The operating climate (financial stability, competitors, pace of technological change, market trends, etc).

Understanding the specific organisation:

- Structure and organisation.
- Reporting and accountability relationships.
- Internal standing financial orders/regulations etc.
- Key people (Senior management team, operational staff, etc).

1 mark per relevant point made up to maximum of 4

(7)

(d) (i) Audit needs assessment

The audit plan should be based on prioritisation of relative risks of auditable activity. The audit risk approach includes consideration of risks outside the direct control of auditors:

Inherent risk - the risk that errors will arise as a result of the business environment; examples may include a volatile market, new company set up, complex legislative requirements.

Control risk - the risk that internal controls will fail to prevent errors from occurring or fail to detect them if they do occur; examples may include inadequate segregation of duties, insufficient management review (say of budget/actual information).

1 mark each for definition of inherent/control risk and relevant example up to maximum of 4

(ii) Risk indexation approach

Advantages:

- Less subjective than relying on judgement of auditors.
- Good for financial or quantitative systems.
- Promotes a more thorough approach (taking account of a range of elements of risk).
- Can be used to justify audit coverage to management/auditees.
- Helpful for new organisations/inexperienced management.

Disadvantages:

- Time and resource intensive in collection of data/information to support scores.
- May be difficult to obtain data required, or for non-quantitative activities.
- Still a large degree of subjectivity (e.g. choice of approaches, relative weightings, etc).

1 mark per relevant point on risk indexation up to maximum of 3

(7)

(e) Risks associated with contracts

Cost overruns on budget owing to:
- Variations from original specification (may not be subject to same level of scrutiny before authorisation).
- Poor controls over stage payments (eg lack of retention moneys).

Time overruns which may lead to:
- Loss of revenue (eg late opening of leisure centre means lost income).
- Failure to provide service (Could lead to financial loss if compensation due to users).
- Knock on effects on other services or parts of the organisation (eg lack of access to new IT systems).

Failure to enforce penalties
- Lack of terms in contract (eg no liquidated damages or provision for arbitration).
- Unwillingness to take on contractors (may send out signals to contractors that they will not suffer for failing to meet terms).

Risk of fraud or corruption
- Deliberate abuse of contract by contractor (eg charging for work not in fact done).
- Possibility of corruption on part of officials (eg bribes for preferred treatment).

Risks to Value for Money
- Poor specification leading to waste or extravagance.
- Failure to properly identify objectives/requirements.
- Lack of suitable contractors (no competition; no experience; poor financing).

Risks to reputation
- Bad publicity/poor public opinion.
- Adverse EA reports (VFM reports; reports in the public interest).

Failure to learn from mistakes leading to mistakes being repeated.

1 mark for each risk clearly and fully explained up to maximum of (4)

(f) Contract Audit

Contract audit should focus on three key stages - pre-contract, currency of the contract and post contract.

Candidates may suggest a wide range of possible controls in place at each stage of the contract audit process. Examples of typical controls are included below:

Pre-contract

- The feasibility of different options should be assessed.
- A model bid should be prepared to assist budget setting and to help assess the reasonableness of bids.
- European legislation should be complied with.
- No informal communication between officers and contractors.
- Tenders to be received in sealed, unmarked envelopes.
- Receipt of each envelope to be recorded in a register and each envelope date stamped.
- Unopened tenders to be stored securely.
- Late tenders not accepted after other tenders opened.
- Tenders to be opened by two officers independent of the invitation process.
- The reasonableness of bids to be checked by technically competent officers (compare with model bid).
- Tender acceptance should be formal and in writing.

Currency of contract

- An overall capital/budget programme profiled over the year and monitored monthly.
- Prompt recording of expenditure.
- The valuation of work in progress.
- The contract register to record the tender price and each payment as it is made.
- A Valuer/Quantity Surveyor (for capital works) to value work done and to certify a valuation certification before payment is made.
- Rates/prices on invoices to be checked to tender documents.
- 5%-10% retention on each payment.
- The work to be monitored by a technically skilled officer against an agreed “critical” tasks plan.
- Annual price fluctuations to be laid down in the contract (e.g. RPI).
- All variations priced according to a bill of quantities or at an agreed standard rates.

Post contract

- Practical Completion Certificate issued when technical officers assess work is practically complete. Issued with a "snag list" (capital contracts).
- Final invoices checked and certified by the valuer before payment is made.
- Certificate of Practical Completion to be compared with agreed completion date recorded in controls register.
- Major contracts to be reported to Members/Board on completion. Report to consider:
  - actual vs. planned completion date,
  - actual cost vs. budget,
  - description of problems encountered,
  - assessment of lessons learned during the project, and
  - assessment of the contractor.
- Assessment after a set period of whether objectives of the project have been met

1 mark per example control, up to a maximum of 3 in each area

(9)

(g) External Audit reliance on the work of Internal Audit

External audit should review the internal audit function. A favourable assessment might allow the external auditors to modify the nature, timing and extent of external audit procedures.

External audit should consider the following areas as part of their review:

- The Organisational Status of Internal Audit as this affects its ability to be objective. Reporting lines and any requirement to do non-audit duties affects this.
- The Scope of Internal Audit which should be formally stated and should cover all aspects of the client's activities. The review may also consider how management act on internal audit recommendations.
- Whether Due Professional Care is exercised by Internal Audit. To assess this planning, recording and control of individual audit tasks may be reviewed. The existence of adequate audit manuals, work programmes and working papers may be considered.
- The Technical Competence of Internal Audit. This can be assessed by reviewing the qualifications and experience of the audit team along with an assessment of on-going training arrangements.

1 mark for explanation of benefit of cooperation and 1 mark for each component of IA review, up to an overall maximum of (5)

(40)

Question 2

(a) Responsibilities for fraud and misconduct

Management

- Primary responsibility for the prevention and detection of fraud.
- Take steps to provide reasonable assurance that the activities of the entity are conducted honestly and that assets are safeguarded.
- Establish arrangements designed to deter fraudulent or other dishonest conduct.
- Ensure that to the best of their knowledge and belief, financial information, whether used in the entity or for financial reporting is reliable.

External audit

- Should design audit procedures so as to have a reasonable expectation of detecting misstatements arising from fraud or error which are material to the financial statements.
- Where a suspected fraud is identified, all reasonable suspicions should be reported to an appropriate level of management.
- External auditors should consider the extent of fraud and whether it materially affects the financial statements.

Internal audit

- Role in regard to fraud determined by management.
- Should have sufficient knowledge to identify the indicators of fraud.
- Not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.
- Should plan work and design testing with regard to the possibility that fraud may occur.
- Control weakness which might allow fraud to take place to be highlighted to management.
- Evidence or reasonable suspicions of fraud should be reported to the appropriate level of management.

1 mark for each relevant point up to maximum of (9)

(b) Key steps for initial investigation of suspected fraud

- Immediately record the facts that gave rise to the suspicion.
- If cash is involved, count it immediately in the presence of the suspect and another auditor or officer of the organisation.
- Consult the audit manager for advice.
- Report the matter to the management of the organisation.
- Retain securely all documentary evidence; originals not photocopies.

1 mark for each relevant point up to maximum of (4)

(c) Consideration of evidence

- Consideration of **sufficiency** of evidence - how much does the auditor need?
- Sufficiency should be judged in context of the level of assurance required and the scope or extent of the procedures adopted.
- Consideration of the **relevance** of evidence - the audit evidence must relate to a specific audit objective for the amount or system under examination.
- Consideration of the **reliability** of evidence - considering that evidence obtained by the auditor directly is usually the most reliable form of evidence, with evidence from third parties then being second most reliable and in preference to evidence from the client organisation.

Other factors affecting reliability include:

- Documentary evidence is unusually more reliable than oral evidence.
- Evidence obtained form a reliable control environment is likely to be more reliable than that obtained in the context of an unreliable control environment
- Less complex audit procedures are often more reliable than complex ones.
- If auditors have to rely on assertions from management, corroborative evidence should be sought where possible from outside sources.
- Verbal assurances should be confirmed in writing to remove possibilities of misunderstanding.

1 mark for each relevant point up to maximum of (7)

(20)

Question 3

(a) Three aspects of materiality

3 aspects of materiality to be considered by external auditors:

Materiality by value - a monetary amount to be treated as the upper tolerable limit on the value of any error found during audit fieldwork. Examples may include percentage values of organization wide activity (e.g. turnover) or of specific activities (e.g. assets, sales).

Materiality by nature – errors which are considered material by virtue of their high profile or of the specific disclosures expected of them, which may be regardless of the monetary value of the error. Examples may include the impact of fraudulent activity in the public sector (for which stakeholders may have more sensitivity than in the private sector) or categories such as the audit fee or directors' remuneration) which require separate notes in accounts.

Materiality by context - which considers the impact of the error on the view, use or interpretation of the financial statements. Examples may include an error which, if corrected, would turn a surplus into a deficit.

Up to 2 points for each category, illustrated by example, up to maximum of (6)

(b) Financial statements assertions

ISA 500 distinguishes three categories of assertion and the detailed objectives in each categories:

Assertions about classes of transactions and events for the period under audit:

Detailed objectives may include:

Occurrence - transactions and events that have been recorded have occurred and pertain to the entity.
Completeness - all transactions and events that should have been recorded have been recorded.
Accuracy - amounts and other data relating to recorded transactions and events have been recorded appropriately.
Cut-off - transactions and events have been recorded in the correct accounting period.
Classification - transactions and events have been recorded in the proper accounts.
Regularity - (for public sector, APB PN10) expenditure is in accordance with authorizing legislation and money has been applied for the purposes intended.

Assertions about account balances at the period end:

Existence - assets and liabilities exist.
Completeness - all assets and liabilities that should have been recorded have been recorded.
Rights and obligations - the entity holds or controls the rights to assets and liabilities are the obligations of the entity.
Valuation and allocation - assets and liabilities are included in the financial statements at appropriate amounts and any resulting valuation or allocation adjustments are appropriately recorded.

Assertions about presentation and disclosure:

Occurrence and rights and obligations - disclosed events, transactions and other matters have occurred and pertain to the entity.
Completeness - all disclosures that should have been included in the financial statements have been included.
Classification and understandability - financial information is appropriately presented and described, and disclosures are clearly expressed.
Accuracy and valuation - financial and other information are disclosed fairly and at appropriate amounts.

Up to 2 points for each category and example objective, up to maximum of (6)

(c) External audit opinions

External auditors may qualify their opinion on the basis of:

- Limitation of scope of the auditors work; for example imposed by management, circumstances outside the auditor's control or resulting from inadequate accounting records.
- Disagreement with management regarding the acceptability of the accounting policies selected, the method of their application or adequacy of disclosures.

Auditors assess the matter as :-

- Material - the omission or misstatement would reasonably influence the decisions of a user of the financial statements.
- fundamental - it is so material or pervasive that the financial statements are seriously misleading.

The resulting audit opinion:

	Limitation of scope	**Disagreement**
Material	Qualified "except for" - describe the circumstances of the limitation of scope	Qualified "except for" - describe the basis of the disagreement
Fundamental	Disclaimer	Adverse opinion

Up to 1 mark for each basis of qualification and basis of assessment up to maximum of 4
Up to ½ mark for each opinion correctly allocated to circumstances up to maximum of 2

(6)

(d) Significant uncertainty

This is a matter whose outcome depends on future actions or events not under the direct control of the entity, but which may affect the financial statements. The uncertainty will be resolved at a future date when more information becomes available. Examples used to illustrate the definition may include future recoverability of a major debtor, major legal actions, etc.

Up to 1 mark for each point clearly and fully explained, up to maximum of (2)

(20)

Question 4

(a) Inherent risks in the use of IT

- Natural disaster: e.g. power loss, lightning storms, flood, fire. Risks to both hardware and data.
- Breakdown: systems far more reliable than in past but also more complex and, due to ubiquity, loss of IT can be disastrous to day to day activities, front line services etc.
- Physical security: IT equipment is becoming more portable, giving rise to risk of loss/theft. Also risk of theft or changes to data.
- Environmental risks: Less of an issue than before (old mainframe systems rather sensitive pieces of kit) but some larger computers can require special environment to reduce risks from heat, water, fire etc.
- Internet/virus attack: Risks of viruses and similar, remote hacking and inappropriate/illegal use of internet.

Up to 1 mark for each risk clearly and fully explained up to maximum of (4)

(b) IT controls to address specific concerns

(i) Appropriate **management controls** should be established to meet the concerns arising from the formation of the new team. These controls should include

- Establishing overall responsibility for IT and developing an IT security policy.
- Ensuring staff are adequately trained.
- Organising the IT service appropriately (ie to avoid duplication/gaps in services and reduce risk that service failures / interruptions may occur).
- Establish effective segregation of duties (eg access to live systems restricted).

(ii) **Internet controls** - Appropriate internet use should be defined and documented to minimize inappropriate, inefficient and insecure activities. A policy on use should be developed and communicated to all staff, with procedures in place to monitor, detect and act on inappropriate use. IT systems should be protected by virus protection software and firewalls.

(iii) **Network controls** (to minimize network failure) may include regular monitoring and maintenance of the network, insurance, regular back-up of both software and data and (in the event of a failure) appropriate recovery and business continuity plans.

(iv) **File access controls** may include:

- Use of passwords (with minimum length, required format, required change functionality).
- Access rights to files appropriate to role and only set up after appropriate authorisation.
- Software facilities such as timeout and logout to reduce risk on unauthorized access.
- Monitoring of file access by systems software and all attempted violations investigated by management.

(v) **PC controls** should be established which may include:

- Laptops to be allocated to specific staff (and documented records maintained).
- Laptops to be stored to minimise risk of theft.
- Password protection (and user identification) to control access to information.
- Prevention of installation of other software.
- Requirement for regular back up of data.

Up to 1 mark for each appropriate control in each of the categories above, subject to a maximum of 2 marks per scenario

(10)

(c) (i) Benefits of use of CAATs

- Increased extent of audit testing (possibly up to 100% sampling) which can reduce sampling risk.
- Speed and accuracy of procedures.
- Performing manually impossible tasks (e.g. in the absence of audit trail or manual record).
- Cost effectiveness, for example in use of tools/techniques in subsequent years. This can be expressed as a benefit for both the auditor and auditee.
- Elimination of repetitive work, increasing time for judgemental aspects of the audit.
- Increased knowledge of client systems.

(ii) Examples of CAATs

- Data retrieval.
- Test data.
- Parallel simulation.
- Embedded audit modules.
- Program review.
- Program comparison.

1 mark for each benefit outlined, up to a maximum of 4, with 1 further mark for each example of CAATs fully explained, up to a maximum of 2

(6)

(20)

Question 5

(a) Risk management is concerned with evaluating the measures the organisation already has in place to manage identified risks and then recommending action that the organisation needs to take to control these risks more effectively.

When confronted by risk, there are four courses of action from which to choose:

- Control (or treat) the risk.
- Live with (or tolerate) the risk.
- Insure against (or transfer) the risk.
- Terminate the activity.

1 mark for appropriate definition of risk management; up to 1 mark for each option, clearly and fully explained, with appropriate illustration. Maximum of (5)

(b) (i) The core purpose / function of the audit committee may include:

- Approval but not direction of the authority's internal audit strategy, plan and performance.
- Review summary internal audit reports and main issues arising, and seek assurance that appropriate action has been taken.
- Consider the reports of external audit and inspection agencies.
- Consider the effectiveness of the authority's risk management arrangements, the control environment and associated anti-fraud and anti-corruption arrangements.
- Be satisfied that the authority's assurance statements, including the Statement of Internal Control, properly reflect the risk environment and any actions required to improve it.
- Ensure that there are effective relationships between IA and EA, inspection agencies and other relevant bodies, and that the value of audit activity is promoted.
- Review the financial statements, EA opinion and reports to members and monitor management action in response to EA issues.

1 mark for each feature, plus 1 mark for explanation of impact on effectiveness, up to a maximum of (5)

(ii) Features for the effective operation of the audit committee may include

- Strong chair, displaying a depth of skills and interest.
- Unbiased attitudes, treating auditors, the executive and management equally.
- The ability to challenge the Executive (e.g. Leader, Chief Executive) when required.
- A membership that is balanced, objective, independent of mind and knowledgeable.

1 mark for each feature, plus 1 mark for explanation of impact on effectiveness, up to maximum of (4)

(c) COSO internal control framework

- Control environment – factors such as the integrity, ethical values and competence of the people working in the organisation and the attention and direction of the board of directors to such matters.
- Risk assessment – the identification, assessment and management of risk.
- Control activities – the internal control procedures established by management to direct activities, for example including segregation of duties, approval, authorisation, verification, reconciliation, management review and security of assets.
- Information and communication - correct, timely information to the correct recipient. For example, including staff awareness of responsibilities, documented policies and procedures, and communication with external 'stakeholders'.
- Monitoring - internal control systems need to be monitored, to assess the quality of performance over time.

The components need to be defined by senior management. The categories of control and the five components overlap and are intertwined. This illustrates that the internal control framework needs to be built into the wider systems and processes utilized by the organisation

1 mark for each component and explanation of the framework, up to maximum of (6)

(20)