PAPER P3

PERFORMANCE STRATEGY

Acorn Chapters

Syllabus overview

Two key issues underpin Paper P3 – what risks does the organisation face and how can those risks be managed and controlled? The scope of the paper includes both financial and non-financial risks. The management strategies covered extend to the use of financial instruments, and more general strategies of risk identification and management, involving establishing and monitoring appropriate systems of internal control. With the growing importance of 'new' sources of risk, the paper pays particular attention to risks arising from governance, ethical and social/environmental issues.

Syllabus structure

The syllabus comprises the following topics and study weightings:

A	Management Control Systems	10%
B	Risk and Internal Control	25%
C	Review and Audit of Control Systems	15%
D	Management of Financial Risk	35%
E	Risk and Control in Information Systems	15%

Assessment strategy

There will be a written examination paper of three hours, plus 20 minutes of pre-examination question paper reading time. During the 20 minutes you can: read the question paper and annotate or highlight the question paper. However you will not be allowed to: open the answer book; write in the answer book; add any loose sheets/supplements to your answer book; or use calculators. Failure to comply with these rules will be considered as a serious breach of the exam regulations.

The examination paper will have the following sections:

Section A	50 marks	A maximum of four compulsory questions, all relating to a pre-seen case study and further new unseen case material provided in the examination. (Note: The pre-seen case study is common to all three of the strategic level papers at each examination sitting i.e. Paper E3, P3 and F3).
Section B	50 marks	Two questions, from a choice of three, each worth twenty five marks. Short scenarios will be given, to which some or all questions relate.

A. MANAGEMENT CONTROL SYSTEMS (10%)

1. evaluate control systems for organisational activities and resources.

(a) evaluate appropriate control systems for the management of an organisation;

(b) evaluate the appropriateness of an organisation's management accounting control systems;
(c) evaluate the control of activities and resources within an organisation;

(d) recommend ways in which identified weaknesses or problems associated with control systems can be avoided or solved.

• The ways in which systems are used to achieve control within the framework of an organisation (e.g. contracts of employment, policies and procedures, discipline and reward, reporting structures, performance appraisal and feedback).

• The application of control systems and related theory to the design of management accounting control systems and information systems in general (i.e. control system components, primary and secondary feedback, positive and negative feedback,
open and closed-loop control).

• Structure and operation of management accounting control systems (e.g. identification of appropriate responsibility and control centres within the organisation, performance target setting, avoiding unintended behavioural consequences of using management accounting controls).

• Variation in control needs and systems dependent on organisational structure (e.g. extent of centralisation versus divisionalisation, management through strategic business units).

• Assessing how lean the management accounting system is (e.g. extent of the need for detailed costing, overhead allocation and budgeting, identification of non-value adding activities in the accounting function).

• Cost of quality applied to the management accounting function and "getting things right first time".

B. RISK AND INTERNAL CONTROL (25%)

1. evaluate types of risk facing an organisation.

(a) discuss ways of identifying, measuring and assessing the types of risk facing an organisation, including the organisation's ability to bear such risks;

(b) evaluate risks facing an organisation.

• Types and sources of risk for business organisations: financial, commodity price, business (e.g. from fraud, employee malfeasance, litigation, contractual inadequacy, loss of product reputation), technological, external (e.g. economic and political), and corporate reputation (e.g. from environmental and social performance or health and safety) risks.
• Fraud related to sources of finance (e.g. advance fee fraud and pyramid schemes).
• Risks associated with international operations (e.g. from cultural variations and litigation risk, to loss of goods in transit and enhanced credit risk). (Note: No specific real country will be tested).
• Quantification of risk exposures (impact if an adverse event occurs) and their expected values, taking account of likelihood.
• Information required to fully report on risk exposures.
• Risk map representation of risk exposures as a basis for reporting and analysing risks.

2. evaluate risk management strategies and internal controls.

(a) discuss the purposes and importance of internal control and risk management for an organisation;

(b) evaluate risk management strategies;

(c) evaluate the essential features of internal control systems for identifying, assessing and managing risks;

(d) evaluate the costs and benefits of a particular internal control system.

• Purposes and importance of internal control and risk management for an organisation.
• Issues to be addressed in defining management's risk policy.
• The principle of diversifying risk. (Note: Numerical questions will not be set).
• Minimising the risk of fraud (e.g. fraud policy statements, effective recruitment policies and good internal controls, such as approval procedures and separation of functions, especially over procurement and cash).
• The risk manager role (including as part of a set of roles) as distinct from that of internal auditor.
• Purposes of internal control (e.g. safeguarding of shareholders' investment and company assets, facilitation of operational effectiveness and efficiency, contribution to the reliability of reporting).
• Elements in internal control systems (e.g. control activities, information and communication processes, processes for ensuring continued effectiveness etc).
• Operational features of internal control systems (e.g. embedding in company's operations, responsiveness to evolving risks, timely reporting to management).
• The pervasive nature of internal control and the need for employee training.
• Costs and benefits of maintaining the internal control system.

3. evaluate governance and ethical issues facing an organisation.

(a) discuss the principles of good corporate governance, particularly as regards the need for internal controls;
(b) evaluate ethical issues as a source of risk to the organisation and control mechanisms for their detection and resolution.

• The principles of good corporate governance based on those for listed companies (the Combined Code), e.g. separation of chairman and CEO roles, appointment of non-executive directors, transparency of directors' remuneration policy, relations with shareholders, the audit committee. Other examples of recommended good practice may include The King Report on Corporate Governance for South Africa, Sarbanes-Oxley Act in the USA, The Smith and Higgs Reports in the UK, etc).
• Recommendations for internal control (e.g. The Turnbull Report).

• Ethical issues identified in the CIMA Code of Ethics for Professional Accountants, mechanisms for detection in practice and supporting compliance.

C. REVIEW AND AUDIT OF CONTROL SYSTEMS (15%)

1. discuss the importance of management review of controls.

(a) discuss the importance of management review of controls.

• The process of review (e.g. regular reporting to management on the effectiveness of internal controls over significant risks) and audit of internal controls.
• Major tools available to assist with a review and audit process (e.g. audit planning, documenting systems, internal control questionnaires, sampling and testing).

2. evaluate the process and purposes of audit in the context of internal control systems.

(a) evaluate the process of internal audit and its relationship to other forms of audit;
(b) produce a plan for the audit of various organisational activities
including management, accounting and information systems;
(c) recommend action to avoid or solve problems associated with the audit of activities and systems;
(d) recommend action to improve the efficiency, effectiveness and control of activities;
(e) discuss the relationship between internal and external audit work.

• Role of the internal auditor and relationship of the internal audit to the external audit.
• Relationship of internal audit to other forms of audit (e.g. value-for-money audit, management audit, social and environmental audit).
• Operation of internal audit, the assessment of audit risk and the process of analytical review, including different types of benchmarking, their use and limitations.
• Particular relevance of the fundamental principles in CIMA's Ethical Guidelines to the conduct of an impartial and effective review of internal controls.
• Detection and investigation of fraud.
• The nature of the external audit and its process, including the implications of internal audit findings for external audit procedures.

3. discuss corporate governance and ethical issues facing an organisation.

(a) discuss the principles of good corporate governance for listed companies, for conducting reviews of internal controls and reporting on compliance;
(b) discuss the importance of exercising ethical principles in conducting and reporting on internal reviews.

• The principles of good corporate governance for listed companies, for the review of the internal control system and reporting on compliance.
• Application of the CIMA Code of Ethics for Professional Accountants to the resolution of ethical conflicts in the context of discoveries made in the course of internal review, especially section 210.

D. MANAGEMENT OF FINANCIAL RISK (35%)

1. evaluate financial risks facing an organisation.

(a) evaluate financial risks facing an organisation.

• Sources of financial risk, including those associated with international operations (e.g. hedging of foreign investment value) and trading (e.g. purchase prices and sales values).
• Transaction, translation, economic and political risk.

• Quantification of risk exposures, their sensitivities to changes in external conditions and their expected values.

2. evaluate alternative risk management tools.

(a) evaluate appropriate methods for managing financial risks;
(b) evaluate the effects of alternative methods of risk management;
(c) discuss exchange rate theory and the impact of differential inflation rates on forecast exchange rates;
(d) recommend risk management strategies and discuss their accounting implications.

• Minimising political risk (e.g. gaining government funding, joint ventures, obtaining local finance).
• Operation and features of the more common instruments for managing interest rate risk: swaps, forward rate agreements, futures and options. (Note: Numerical questions will not be set involving FRA's, futures or options. See the note below relating to the Black Scholes model).
• Operation and features of the more common instruments for managing currency risk: swaps, forward contracts, money market hedges, futures and options. (Note: The Black Scholes option pricing model will not be tested numerically, however, an understanding of the variables which will influence the value of an option should be appreciated).
• Simple graphs depicting cap, collar and floor interest rate options.
• Theory and forecasting of exchange rates (e.g. interest rate parity, purchasing power parity and the Fisher effect).
• Principles of valuation of financial instruments for management and financial reporting purposes (IAS 39), and controls to ensure that the appropriate accounting method is applied to a given instrument.
• Quantification and disclosure of the sensitivity of financial instrument values to changes in external conditions.
• Internal hedging techniques (e.g. netting and matching).

E. RISK AND CONTROL IN INFORMATION SYSTEMS (15%)

1. evaluate the benefits and risks associated with information related systems .

(a) advise managers on the development of information management (IM), information systems (IS) and information technology (IT) strategies that support management and internal control requirements;
(b) evaluate IS/IT systems appropriate to an organisation's needs for operational and control information;
(c) evaluate benefits and risks in the structuring and organisation of the IS/IT function and its integration with the rest of the business;
(d) recommend improvements to the control of IS;
(e) evaluate specific problems and opportunities associated with the audit and control of systems which use IT.

• The importance and characteristics of information for organisations and the use of cost-benefit analysis to assess its value.
• The purpose and content of IM, IS and IT strategies, and their role in performance management and internal control.
• Data collection and IT systems that deliver information to different levels in the organisation (e.g. transaction processing,
decision support and executive informative systems).
• The potential ways of organising the IT function (e.g. the use of steering committees, support centres for advice and help desk facilities, end user participation).
• The arguments for and against outsourcing.
• Methods for securing systems and data back-up in case of systems failure and/or data loss.

- Minimising the risk of computer-based fraud (e.g. access restriction, password protection, access logging and automatic generation of audit trail).
- Risks in IS/IT systems: erroneous input, unauthorised usage, imported virus infection, unlicensed use of software, theft, corruption of software, etc.
- Risks and benefits of Internet and Intranet use by an organisation.
- The criteria for selecting outsourcing/facilities management partners and for managing ongoing relationships, service level agreements, discontinuation/change of supplier, hand-over considerations.
- Controls which can be designed into an information system, particularly one using IT (e.g. security, integrity and contingency controls).
- Control and audit of systems development and implementation.
- Techniques available to assist audit in a computerised environment (computer-assisted audit techniques e.g. audit interrogation software).