

MOCK TEST PAPER
FINAL (NEW) COURSE: GROUP – II
PAPER – 6A: RISK MANAGEMENT

Solutions

Note: Please note these solutions are for guidance purpose only.

ANSWERS TO CASE STUDY: 1

1.1 A measure that covers the entire following requirement is Altman Z Score.

- (i) Quantum of Liquid Assets in relation to the size of the company.
- (ii) Profitability of the company reflecting the company's age and earning power.
- (iii) Operating Efficiency apart from tax and leveraging factors.
- (iv) Market dimensions that can show up security price fluctuations as a possible red flag.
- (v) Total Asset Turnover.

The original Z-score formula was as follows:

$$Z = 1.2X_1 + 1.4X_2 + 3.3X_3 + 0.6X_4 + 1.0X_5$$

X_1 = working capital / total assets. Measures liquid assets in relation to the size of the company.

X_2 = retained earnings / total assets. Measures profitability that reflects the company's age and earning power.

X_3 = earnings before interest and taxes / total assets. Measures operating efficiency apart from tax and leveraging factors. It recognizes operating earnings as being important to long-term viability.

X_4 = market value of equity / book value of total liabilities. Adds market dimension that can show up security price fluctuation as a possible red flag.

X_5 = sales / total assets. Standard measure for total asset turnover (varies greatly from industry to industry).

For the various figures required in above formula let us reproduce the Balance Sheet as follows:

INR (Rs.) Thousand

Liabilities		Amount	Assets	Amount
Share Capital	222,248		Total Fixed Assets	214,666
Profit & Loss A/c	61,549		Total Current Assets	679,539
Other Reserve	36,303		Total Non-Current Assets	70,838
Less: Intangibles	9,620	310,480		
Minorities		62,929		
Provision/ Other Long Term Loans		56,445		
Bank O/D and Short Term Loans		1,52,281		
Current Liabilities		382,908		
		9,65,043		9,65,043

Other Data:

Working Capital = 679,539 – 382,908 – 152,281 = 144,350

EBIT = 93,410

Retained Earnings = 65,550

Sales = 1,469,762

Market Value of Equity = 80.70 x 22,224.80 = 1,793,541.36

Altman Z Score

$$= 1.2 \times \frac{158,743}{965,043} + 1.4 \times \frac{65,550}{965,043} + 3.3 \times \frac{93,410}{965,043} + 0.6 \times \frac{1,793,541.36}{965,043} + 1.0 \times \frac{14,69,76}{965,043}$$

$$= 0.1974 + 0.0951 + 0.3194 + 1.1151 + 1.523 = 3.25$$

Since the Altman Z Score is 3.25 there is Negligible Risk of bankruptcy.

Note: There may be slight variation in the answer due to difference in considering the items to be included in the various sums used in the formula.

1.2 (D)

1.3 (C)

1.4 (D)

1.5 (C)

1.6 (B)

ANSWERS TO CASE STUDY: 2

2.1 Risk Report of Ms. X has following shortcomings:

- (1) All Risks have been categorised as Operational Risks which is wrong.
- (2) Bucketing of risk is incorrect and that too not supported by reasons.

Revised Report

To: Board of Directors

From: Chartered Accountant

Date: -----

Subject: Grading/ Bucketing of Various Risks

Introduction

This report covers grading/ bucketing of various identified risks.

Grading of various Risks

- (1) Stagnant business growth resulting from competition from other airlines.

Although this risk has a high impact but has low probability as investment involved in the Airline business is very huge. Accordingly, this risk often skips the management's decision as these type events cannot be foreseen. Hence, this risk is bucked in the category of '**High Impact – Low Probability**'.

- (2) Aggressive fleet expansion leading to over-capacities.

Since Airline has already ordered 170 aircrafts there is high probability that it will involve financial commitments and impact will also be high. Hence, this risk is bucked in the category of '**High Impact – High Probability**' and it needs immediate and sufficient attention of management.

(3) Safety Standards resulting in Crash/ disastrous hijacking

Any crash or dangerous hijacking incidents will create negative publicity, poor image resulting in a decline in revenue and similar consequences.

Whilst the probability is low, the strong impact ought to force the seeking of appropriate mitigants. Hence, the impact is high and can be classified as '**Low Probability – High Impact**'. It is suggested to ensure the adequacy of safety systems, to establish the average age of the aircraft and if necessary, to seek the help of an external expert.

(4) Volatile Oil Prices

Oil price fluctuation is a business risk that has serious implications for the profitability of the airline business. However, since this affects almost all competitors, the impact can be considered as low and can be categorized as '**Low Probability – Low Impact**'.

Signed/-

Chartered Accountant

2.2 (A)

2.3 (B)

2.4 (A)

2.5 (B)

2.6 (A)

ANSWERS TO CASE STUDY: 3

3.1 Report to Board of Directors

To: The Board of Directors, ABC Co. Ltd.

From: Chief Risk Officer

Date: 30 April 2021

Subject: Analytical Report on Risks Involved

This analytical report covers the reply on the various concerns raised by the Board of Directors.

(a) What is the type of the risk the Company is subject to?

The risk arising from this lapse is 'Legal Risk' or 'Compliance Risk' as it is resulting from the failure to comply with statutory or legal requirements.

(b) Impact on Company's Performance

The various types of impacts on the company's performance are as follows:

- (i) Bringing bad name and reputation for the Company.
- (ii) Over or Under Statement of Profit Loss in Income Statement of Company leading wrong decisions by the Company itself and external parties.
- (iii) Wrong financial position of the Company in the Balance Sheet.
- (iv) Due to wrong calculation of profit company may have paid wrong dividend in previous years.
- (v) Wrong computation of Cash Flows of the previous years and consequently leading to wrong budgeting figures.
- (vi) Wrong decision based on wrong budgeted figures.

Signed/-

Chief Risk Officer

3.2 (B)

3.3 (B)

3.4 (A)

3.5 (D)

3.6 (C)

ANSWERS TO CASE STUDY: 4

4.1 There are several specific aspects that need to be looked into Outsourcing Risk. Hiring of an outsourced vendor/service provider must cover the following aspects:

- Clearly defined objective of outsourcing; this has to be brought into the scope of work;
- Contractual documentation to be adequate to ensure the service provider does only what is assigned and to the standard mutually agreed to by all parties involved;
- Legal indemnities to the organisation to be assessed while hiring a service provider;
- In agreements where the client and the service provider are in different states or in different countries, the respective countries' or states' laws have to be complied with;
- The BCP of the service provider has to be reviewed.
- The operational risk assessment covering regulatory risks, financial risk, financial reporting risk and other risks as delivery to end customers of the client in case the service provider fails to deliver for whatever reason.
- If technology or its disaster recovery itself is outsourced, all the attention is required to ensure the business operations work as designed and agreed.

4.2 From an auditor's perspective or the operational risk professional perspective, the main issues that can surface from technology risk are:

- (a) **Unscheduled system downtime:** Also called system malfunctioning due to which a business process is disrupted, due to which the necessary work output suffers a setback. This could result in financial loss, loss of opportunity of business, customer issues and loss of raw material. For example, a system failure in a financial lending organisation may lead to critical customer commitments like disbursements not happening due to which customer may suffer losses; or inability to post incoming payments on account leading to liquidity issues; or inability to service a customer account leading to customer attrition. Organisations have backup servers, systems, databases, and disaster recovery procedures to ensure work disruption is minimized in such circumstances. The operational risk manager is expected to have an overview of the specific facilities available to the technology department, to service the organisation's critical needs at such times of failure.
- (b) **System failure pertaining to incorrect programming:** This is by far the most common cause of operational risk events in an organisation, since each system can only function in the manner it is set up. Organisations either build their own systems or buy them from specialised service providers, and customise them. In either case, depending on the nature of transactions required to be processed, a very detailed business requirement document is required to be given to the technology department by the business user groups. Often, either due to incapability or poor co-ordination between the business user groups, the requirement document does not capture the entire detailing and the extremely granular details that are required by the technical teams doing the coding, customisation or the deployment. The result is a poorly executed system that causes

errors in processing, which may have financial, regulatory, fraud risks, depending on kind of error in the system.

- (c) **Master maintenance:** All systems, besides the basic coding, need a set of Masters which are user-defined parameters that enable the processing of the data. Master configuration is in itself a key risk that technology users face, since the linkages between products or service programs as defined by the business users can be ambiguous, or at times contradictory instructions go to the technology team resulting in erroneous set up of Masters.
- (d) **User access control:** This is by far the most key control in driving controls in an automated controls environment. For example, in a lending institution, a credit officer if allowed to process operational activities beyond his job role may result in compromise of the segregation of duties that the process is designed with; or, if an user may have a higher level of access to changing customer data by one modification, while the process may require an authorisation which was bypassed due to inadequate user access control maintenance. User access control requires the user profiles to be set up properly upfront in the initial basic programming, followed by correct assignment of user profiles upon employee requests as per their permissible authorities basis their job role. Organisations are required to delete or modify user IDs once employees move out from their roles or the organisation itself.
- (e) **Accounting systems:** From an audit and accounting perspective, the most intensive focus area is the technology platform that is used for accounting. There are obvious operational risks of misstatements in financial reporting if the accounting software is not configured properly. In complex organisations with several types of transactions that have a financial impact are performed in various systems, the feed in from other production systems (i.e. outside of the main accounting system) are very important to check for accuracy since they are used in financial reporting. The feeds, if manual have their own risk of incorrect manual processing; in automated feed process also, there are risks of incorrect data inflows that could lead to financial misstatements. In lending institutions, the loan management systems are different from the main accounting system; a huge amount of data, at various frequencies, flows into the accounting system. The linkage of the source system to the correct GLs in accounting system, and appropriate reconciliations, the exception reports, analysis and ongoing supervisory reviews can prevent the data from being inconsistent in final reporting. Any regular exceptions in the data in two systems, need to be analysed to find out the root cause of the technological reason, and any incorrect programming. Examples are the data of customers like interest due, principal outstanding, overdue amounts etc. which flow from loan management systems to accounting systems.
- (f) **Change management:** It is a key area of Information Technology General Controls (ITGC). It simply means that any change to the systems can cause a risk of incorrect change being developed or deployed. This can be a result of multiple causes:
 - Change being carried out without approvals of authorised roles,
 - Change being wrongly conceived by the user groups, without adequate analysis of pros and cons for the change, and getting deployed by the technology unit under approvals
 - Change, though conceived correctly and communicated correctly under adequate approvals to the technology team, is wrongly executed
 - The preventive control around all these issues, is to ensure only authorised roles, whether internal or external, have access to making changes in the system; these changes have to be approved by all the departments that the change impacts so that the impact of change is well understood before approvals are accorded; and, a proper user acceptance testing is conceived and conducted before deploying the change. Often the design of the User Acceptance Testing (UAT) script is found defective, and sufficient combinations of test data

is not put through the system resulting in some functionalities not being adequately tested.

- A database of such changes, such as audit trail reports have to be judiciously maintained as to what changes were carried out, including the issue tracker related to the changes. This helps track back any changes, to ensure that appropriate change management control and review was exercised.
- (g) **Migration risk:** It is a subset of change management ITGC to the extent that the controls over an end-to-end migration from one system to another, can bring upon significant operational risk if not carried out perfectly. A significantly high effort is required to ideate before the deployment as to the exact manner of migration; migration has to cover:
- Data, both dynamic and static
 - Functionality mapping from old to new system, and any changes to be adequately familiarised within user groups
 - Exception reports that could help track any incorrect migration points
 - User acceptance test scripts to be intelligent enough to enable the usage of the new system after adequate granular review
 - An emergency roll back plan in case some significant unpredictable issue comes up in migration deployment.
 - An auditor or operational risk manager is required to carry out a review of the data integrity and the functionality of the systems that have an impact on the financials of the organisation. This risk is not only restricted to financial reporting, but any risk that could jeopardise the business process, including regulatory, financial and other risks.
- (h) **Technology outsourcing risk:** In many organisations the technology platform, or the servicing / maintenance of the platform is outsourced. Outsourcing while has its inherent efficiency benefits comes with operational risks of running a system through a service provider that has no or little understanding of the actual business process the system supports in the organisation; such relationships of principal and service provider have to be carefully defined both contractually as well as from an operational perspective otherwise the seamless functioning of the systems can be disrupted.

4.3 (A)

4.4 (A)

4.5 (A)

4.6 (D)

4.7 (D)

ANSWERS TO CASE STUDY: 5

5.1 RG and other members of the board should:

- (i) Avoid conflicts of interest arising between independent directors, non-executive directors and executive directors.
- (ii) Establish a regular and transparent communication mechanism to ensure continuous and robust dialogue and information sharing between all the board members.
- (iii) Ensure tapping of the maximum benefit of expertise, skills, experience and perspectives of lead independent director.
- (iv) Set the tone from the top, and seek to effectively inculcate an appropriate risk culture throughout the firm.

5.2 The **ICAI Guidance note on Internal Financial Controls** over financial reporting states that for financial reporting purposes, the entity's risk assessment process includes how management identifies business risks relevant to the preparation of financial statements in accordance with the entity's applicable financial reporting framework, estimates their significance, assesses the likelihood of their occurrence, and decides upon actions to respond to and manage them and the results thereof.

For example, the entity's risk assessment process may address how the entity considers the possibility of unrecorded transactions or identifies and analyses significant estimates recorded in the financial statements. Risks relevant to reliable financial reporting include external and internal events, transactions or circumstances that may occur and adversely affect an entity's ability to initiate, record, process, and report financial data consistent with the assertions of management in the financial statements. Management may initiate plans, programs, or actions to address specific risks or it may decide to accept a risk because of cost or other considerations.

Risks can arise or change due to the following circumstances:

- (a) **Changes in operating environment.** Changes in the regulatory or operating environment can result in changes in competitive pressures and significantly different risks.
- (b) **New personnel.** New personnel may have a different focus on or understanding of internal control.
- (c) **New or revamped information systems.** Significant and rapid changes in information systems can change the risk relating to internal control.
- (d) **Rapid growth.** Significant and rapid expansion of operations can strain controls and increase the risk of a breakdown in controls.
- (e) **New technology.** Incorporating new technologies into production processes or information systems may change the risk associated with internal control.
- (f) **New business models, products, or activities.** Entering into business areas or transactions with which an entity has little experience may introduce new risks associated with internal control.
- (g) **Corporate restructurings.** Restructurings may be accompanied by staff reductions and changes in supervision and segregation of duties that may change the risk associated with internal control.
- (h) **Expanded foreign operations.** The expansion or acquisition of foreign operations carries new and often unique risks that may affect internal control, for example, additional or changed risks from foreign currency transactions.
- (i) **New accounting pronouncements.** Adoption of new accounting principles or changing accounting principles may affect risks in preparing financial statements.

5.3 (B)

5.4 (C)

5.5 (A)

5.6 (B)

5.7 (D)