XYZ Limited

Management letter
for the year ended 31 December 2014

Private and Confidential

Board of Directors
XYZ Limited
Mailing address

Date: DD/MM/YYYY

Dear Sirs

Management letter for the year ended 31 December 2014

We set out in the following pages our management letter containing certain matters concerning the internal control, accounting practices and procedures of your company which came to our attention during the course of our audit. In order to facilitate the prioritisation of resources within XYZ Limited to address these observations, we have assigned a risk grading to each observation on the following basis:

Grade	Basis
A	Significant control weakness or business risk that requires immediate management attention.
B	Control weakness that should be included in management's plan to address in the forthcoming year.
C	Matter that is procedural in nature or observation only.

Each point contained in this report is divided into seven sections outlining the following:

- Observation
- Risk
- Exposure rating
- Recommendation
- Management response
- Implementation date
- Individual responsible for the implementation

It is pertinent to mention here that our audit procedures are designed and performed primarily to obtain reasonable assurance about whether the financial statements are free from material misstatements, whether caused by error or other irregularities. Accordingly, we have carried out tests and evaluations of your systems only to the extent necessary for us to decide on reliance to be placed on your procedures and controls in the process of arriving at the above opinion. Thus, such tests and evaluations may not bring to light all the weaknesses that might exist in the systems of internal control and accounting procedures, which a more exhaustive special review of the system might reveal. Please also note fraudulent collusion can override the effectiveness of most controls.

We would like to take this opportunity to express our thanks to the management and staff of the company at all levels for the co-operation and assistance that they have extended to us during the course of our audit.

Please do not hesitate to contact us should you require further clarification regarding any of the matters discussed in this report.

Yours faithfully

Name and signature of audit firm

Table of Contents

1. Core audit

1.1 Maintenance of Fixed Asset Register

Observation

XYZ maintains its Fixed Asset Register (FAR) in excel file which does not contain comprehensive information of the assets (e.g. capitalisation year is recorded instead of capitalisation date). The company calculates its depreciation expense manually based on information contained in FAR.

Risk

Due to maintenance of FAR in excel file, other required fields might be deleted or corrupted at the time of modifying the register. As the FAR does not contain comprehensive information and the Company has a practice to revalue the assets in a regular interval, it might be difficult to ascertain the remaining useful life at the time of revaluation. Moreover, manual calculation of depreciation expense might increase the risk of clerical error leading to an overstatement or understatement of the same.

Exposure rating

A

Recommendation

The Company should initiate prompt action to maintain the fixed asset register in a software system with in-built logic to detect and disallow entries without completing certain fields and which disallows change in useful life of asset without prior approval. Moreover, the system shall contain comprehensive information of assets and calculate the depreciation expense automatically.

Management response

Implementation date

Individual responsible for the implementation

1.2 Asset Identification tag

Observation

During our physical verification of property, plant and equipment, we have observed that none of the assets were tagged with unique asset IDs.

Risk

Absence of asset identification tag leads to the inability of identifying the specific asset from the Fixed Asset Register (FAR). Moreover, this reduces management's ability to track assets including inter-plant transfers and increases the scope for asset misappropriation.

Exposure rating

A

Recommendation

Management should take necessary steps to ensure assets are properly tagged with unique asset IDs.

Management response

Implementation date

Individual responsible for the implementation

1.3 Depreciation policy of the property, plant and equipment

Observation

According to the depreciation policy of the Company, depreciation on additions are charged at 50% of normal rates only in the year of acquisition and no depreciation is charged in the year of disposal.

Risk

As in the first year only half of the annual depreciation is charged and none in the year of disposal, an amount equal to half of the annual depreciation is being left as carrying amount at the time of disposal which leads to a loss on disposal of same amount. Moreover, depreciation charge on new assets could be misappropriated in the year of addition as monthly apportionment of deprecation is not performed. Due to this practice, depreciable amount of an asset is not allocated on a systematic basis over its useful life as per para 50 of IAS 16: *Property, plant and equipment*.

Exposure rating

B

Recommendation

Management should revise its depreciation policy and allocate depreciable amount of assets on a systematic basis over its useful life.

Management response

Implementation date

Individual responsible for the implementation

1.4 Recognition of material in transit for foreign procurement

Observation

XYZ Limited does not recognise material in transit based on the terms and condition of risk and reward transferred as per shipping documents. In most cases, risk and reward is transferred immediately after loading the goods on ship. Material in transit is only recognised on acceptance of L/C documents by the banks or when payment for L/C is made, whichever is earlier, which is generally later than the shipment date.

Risk

Material in transit and corresponding liability might be understated on any cut-off date.

Exposure rating

A

Recommendation

XYZ Limited should recognise the material in transit and corresponding liability on right date (i.e. the date on which the risk and reward is transferred).

Management response

Implementation date

Individual responsible for the implementation

1.5 Payroll reconciliation

Observation

The Confidential department of the Company deals with the payroll payment processing for the employees of the Company where payroll information is updated and salary statement is prepared without any maker checker option embedded in the payroll application. Moreover, in the payroll statement, number of head count is not visible. No monthly payroll reconciliation including joiners' and leavers' information is also performed.

Risk

Due to unavailability of monthly payroll reconciliation and any defined control to review or approve any change of payroll information in the payroll application, error of fraudulent act might be undetected.

Exposure rating

A

Recommendation

Management should implement monthly payroll reconciliation and maker checker methodology in the payroll application to prevent any error, fraudulent and unauthorised changes.

Management response

Implementation date

Individual responsible for the implementation

1.6 Locally procured inventory

Observation

Locally procured inventory, after being received at factory premises and sign off the delivery challan, is kept aside and not booked as asset even though the risk and reward is transferred. The inventory is booked as asset only after the completion of Quality Control (QC) review.

Risk

As most local inventory is procured on credit it is likely that both asset and corresponding liability are understated at any cut-off date.

Exposure rating

B

Recommendation

The inventory shall be booked as asset right after receiving the same and signing off the delivery challan.

Management response

Implementation date

Individual responsible for the implementation

1.7 Foreign exchange gain/loss

Observation

Inventory and capital items procured through L/C are booked after converting foreign currency to BDT using an exchange rate applicable at the date of L/C acceptance and not on the date on which the risk and reward for that asset is transferred.

Risk

Foreign exchange gain or loss is being adjusted with the value of the assets rather than being booked as period cost resulting misstatement of assets and foreign exchange gain/loss.

Exposure rating

B

Recommendation

Management should book assets procured through LC with the exchange rate applicable at the date on which the risk and reward is transferred and should recognise foreign exchange gain or loss accordingly.

Management response

Implementation date

Individual responsible for the implementation

1.8 Foreign revenue

Observation

In case of foreign sales by Pharmaceutical business, revenue is recognised when sales invoice is issued (usually at the time of releasing the goods from depot) rather when actual goods are shipped (usually 2-3 days later from invoice date). As these are foreign sales, revenue should be recognised at the date of shipment (risk and reward are usually transferred on this date) not when invoice is issued.

Risk

Revenue might be understated in a cut-off date.

Exposure rating

B

Recommendation

Revenue should be recognised at the date of shipment of the goods not when invoice is issued.

Management response

Implementation date

Individual responsible for the implementation

1.9 Actuarial valuation of gratuity fund

Observation

As per para 66 of IAS 19: *Employee benefits*), in order to measure the present value of the post-employment benefit obligations and the related current service cost, it is necessary:

- to apply an actuarial valuation method
- to attribute benefit to periods of service
- to make actuarial assumptions

XYZ Limited performs actuarial valuation for the group as a whole and allocates the relevant obligations and current service costs to its subsidiaries on an arbitrary basis. No separate actuarial valuation of gratuity fund for all the relevant subsidiaries of XYZ Limited is performed.

Risk

Leading to misappropriation of relevant post-benefit obligation and expenses among the subsidiaries of XYZ Limited and thus overstating or understating the gratuity provision and expense of these subsidiaries.

Exposure rating

A

Recommendation

It is recommended to perform actuarial valuation for all the relevant components of XYZ Limited individually.

Management response

Implementation date

Individual responsible for the implementation

1.10 Mismatch between deed value and amount paid for land

Observation

The company recognises purchase of land as an asset when legal title is transferred to XYZ and relative control is achieved. During the period, the company purchased land amounting to BDT 300 million in Gazipur. While reviewing deed, it has been noted that the deed value is lower than the amount paid.

Risk

As this leads to non-compliance, legal issues may be imposed by relevant legal authority.

Exposure rating

A

Recommendation

Deed value should be same as amount paid for land purchase to avoid non-compliance and any legal issues.

Management response

Implementation date

Individual responsible for the implementation

2. Control environment

2.1 IT security policy

Observation

XYZ Limited has a documented IT policy for media device, internet, spam mail and related support, but it doesn't cover overall IT security functions viz. password policy, network security policy, disposal of IT equipment.

Risk

In absence of appropriate IT Security policy, the management may find it difficult to identify their security objectives and there is a possibility to lose accountability, integrity and availability of data and other resources.

Exposure rating

A

Recommendation

Management should take steps for implementing a complete and appropriate detailed Information Technology Security Policy.

Management response

Implementation date

Individual responsible for the implementation

2.2 IT security policy awareness training

Observation

XYZ Limited does not conduct information security awareness training. As a result, users are not made adequately aware of the relevant information security policies and practices that need to be followed.

Risk

In absence of IT security policy awareness training, users may inadvertently expose company's information to external threats including information sabotage and virus attacks. Users may also disclose sensitive information to others.

Exposure rating

A

Recommendation

Management should take steps to conduct a proper IT security awareness training for users to inform security issues. User's sign-off should be taken for confirming their understanding on the responsibilities regarding security policies, procedures, acceptable and unacceptable conduct, organisational values and code of ethics.

Management response

Implementation date

Individual responsible for the implementations

2.3 Password configuration

Observation

XYZ Limited is maintaining minimum password length for user. But the Company has not yet implemented periodically password expiry time limit and complexity.

Risk

If password complexity is not enabled and user is not forced to change password periodically, someone else can easily guess simple passwords that can be used to get unauthorised access in the system.

Exposure rating

A

Recommendation

Management should take necessary steps to properly implement password expiry time limit with complexity application in system.

Management response

Implementation date

Individual responsible for the implementation

2.4 Data centre security

Observation

Biometric access system is used to enter data centre. Visitor log book is maintained but it is not reviewed properly. Closed Circuit Camera does not cover data centre fully. Server room of XYZ limited is not neat and clean. Dust and flammable items are also found inside data centre.

Risk

If visitor log register is not reviewed regularly and Closed-Circuit Camera does not cover full area, unauthorised entry into the secured site might not be detected or prevented (there is a chance an outsider can enter in the data centre with internal staff). Flammable items and dust may cause massive loss in data centre.

Exposure rating

A

Recommendation

Management should take steps for reviewing visitor log book regularly (daily or weekly). Closed Circuit Camera should cover full area. Flammable items should be strictly prohibited in data centre. Data centre needs to be cleaned daily and server should be dust free.

Management response

Implementation date

Individual responsible for the implementations

2.5 Disaster recovery site

Observation

XYZ Limited does not have disaster recovery site.

Risk

Any time disaster such as earthquake, fire, tornado, flood, hackers may strike, and then there might be a chance of losing organisational data.

Exposure rating

A

Recommendation

Management should take steps to introduce disaster recovery plan. To implement disaster recovery plan, management needs to build disaster recovery site which should be at least 10 Km radial distance from production site.

Management response

Implementation date

Individual responsible for the implementation

2.6 Change management policy

Observation

XYZ Limited has no change management policy related to software upgrades/changes.

Risk

In the absence of change management policy, various information risks and functions that XYZ Limited needs to manage may not get clear direction, which is a vital factor for success in an organisation with good corporate governance.

Exposure rating

A

Recommendation

XYZ Limited should have approved change management policy which should be reviewed and updated periodically.

Management response

Implementation date

Individual responsible for the implementation

2.7 User acceptance testing

Observation

XYZ Limited does not maintain user acceptance testing for any change in the system.

Risk

Without proper user acceptance form, documentation will remain incomplete. User acceptance is very important to ensure the proper change management implementation in system.

Exposure rating

A

Recommendation

A user acceptance form should be maintained and properly signed by both user and IT personnel to properly document all the requirements and acceptance regarding change management implementation at XYZ Limited.

Management response

Implementation date

Individual responsible for the implementation

2.8 Acquisition and development policy

Observation

There is no approved Software acquisition and development policy adopted by the management.

Risk

Without approved acquisition and development policy, management may face inappropriate developed program releases which may cause program instability.

Exposure rating

A

Recommendation

Management should develop an effective software acquisition and development policy.

Management response

Implementation date

Individual responsible for the implementation

2.9 Incident and problem management

Observation

XYZ Limited does not have incident or problem management procedure, which is a critical business driver for a successful business.

Risk

In absence of incident management procedure enterprise's information security can be damaged if incidents arise from external or internal sources. This may result in financial loss and loss of organisation reputation. Without an effective IT help desk, it could take more time to solve a problem which may cause business loss.

Exposure rating

A

Recommendation

XYZ Limited should develop a charter for incident management which include operational and communication plan. Management should introduce ticketing portal for help desk problem management.

Management response

Implementation date

Individual responsible for the implementation

2.10 Administrator activities monitoring

Observation

XYZ Limited does not practice administrator activities monitoring.

Risk

Without regular monitoring, there is a chance of inappropriate and unauthorised access. This may result in fraudulent activities by the Administrator to remain undetected.

Exposure rating

A

Recommendation

XYZ Limited should practice monitoring of administrator activities at least twice a year.

Management response

Implementation date

Individual responsible for the implementation

2.11 Segregation of duties in purchase order

Observation

Commercial Executive creates PO and according to authorisation limit it is approved, but if any change is required after approval of PO, approver has the authority to edit/change it.

Risk

Without segregation of duties, proper internal control may not be ensured. Also, as control has not been designed, implemented and operated effectively, this may lead to risk of error and misstatements.

Exposure rating

B

Recommendation

XYZ Limited should revoke edit/change authority of approver.

Management response

Implementation date

Individual responsible for the implementation