**From:**Shamme Akhter and Moazzem Hossen

**Date:**7 September 2021

**Subject:** IT Clearance Memo

**To:** Mr. Faruk Uddin Ahammed, Engagement Partner

We are providing a summary of the procedures performed and findings related to certain general IT controls that were tested in connection with the audit of the group financial statements of EPIC Group Limited for the year ended June 30, 2021. As these procedures were specifically performed in support of the audit referenced above, we should consider the information in this memo in determining the extent of any additional procedures that need to be performed in connection with the audit. In addition, as it relates to the performance of this statutory audit, we should consider whether the results of these procedures are relevant for such audit.

Following are the procedures that were performed using International Standards of Auditing (ISA) the requirements of the DTTL Audit Approach Manual and the findings.

**Relevant Application Systems and Technology Elements**

The relevant application systems (including underlying databases and infrastructure) included in our general IT controls testing are as follows:

| **Application System Name(s)** | **Application Description** | **Database** | **Operating System** | **Data Center Location** |
| --- | --- | --- | --- | --- |
| SAP ECC 6.0 Application | Procure to Pay, Order to Cash, Production and Inventory, Property, Plant and Equipment and Period End Financial Reporting | SQL-2008 | Windows Server 2008 | Hongkong |

**Risks Arising from Information Technology (RAITs)**

We identified and assessed RAITs for each application system and associated technology elements stated herein based on our understanding of the role of information technology (IT) in the Group’s flows of transactions, including obtaining an understanding of the IT environment. We identified relevant controls that address the risks for each application system and associated technology elements. The RAITs are as follows.

| **IT Control Area** | **Risk Arising from IT** |
| --- | --- |
| Access Security | Users have access privileges beyond those necessary to perform their assigned duties, which may create improper segregation of duties. |
| Inappropriate changes are made directly to financial data through means other than application transactions. |
| Systems are not adequately configured or updated to restrict system access to properly authorized and appropriate users. |
| System Change Control | Inappropriate changes are made to application systems or programs that contain relevant automated controls (i.e., configurable settings, automated algorithms, automated calculations, and automated data extraction) and/or report logic. |
| Inappropriate changes are made to the database structure and relationships between the data. |
| Inappropriate changes are made to system software (e.g., operating system, network, change-management software, access-control software). |
| Data converted from legacy systems or previous versions introduces data errors if the conversion transfers incomplete, redundant, obsolete, or inaccurate data. |
| Data Center & Network Operations | Individuals gain inappropriate access to equipment in the data center and exploit such access to circumvent logical access controls and gain inappropriate access to systems. |
| Production systems, programs, and/or jobs result in inaccurate, incomplete, or unauthorized processing of data. |
| Financial data cannot be recovered or accessed in a timely manner when there is a loss of data. |
| The network does not adequately prevent unauthorized users from gaining inappropriate access to information systems. |

**Testing of General IT Controls**

We performed the following procedures for general IT controls that were determined to be relevant:

* Determined whether each general IT control, individually or in combination with other controls, is appropriately designed to address the related RAITs.
* Tested the operating effectiveness of relevant general IT controls.
* Considered tools used by the entity in relevant general IT controls and tested controls to address the related risks.
* Obtained audit evidence about the operating effectiveness of relevant general IT controls sufficient to provide a reasonable basis for the conclusions reached.
* We documented and communicated control deficiencies to group management.

**Test result**

We have noted that general IT controls have been tested for the Application and no exceptions was found.

**Conclusion**

As a result of the audit procedures performed, accompanying this communication is a description of any identified deficiencies in internal control over financial reporting for the controls addressed in this memo.

We have determined that the identified RAITs are appropriately addressed during the audit period. Our evaluation was based on our consideration of Chapter 6, "Understanding and Testing General IT Controls," of the *Internal Control Guide*.