AFRC Accounting and Financial Reporting Council 會計及財務匯報局

afrc.org.hk

Checkpoint –

Obtaining an Understanding of the Audit Clients' IT Environments

Inspection **24 January 2025**

In recent years, technology has rapidly transformed the way we live and work. Businesses continue to increase their use of technology, from simple automation to sophisticated, integrated information systems, to improve operational efficiencies, decision-making, customer engagement, and financial reporting. As technology continues to evolve, auditors are recommended to thoroughly understand their audit clients' information systems and communication relevant to the preparation of financial statements.

The Hong Kong Standard on Auditing 315 (Revised 2019) *Identifying and Assessing the Risks of Material Misstatement* (**HKSA 315 (Revised 2019)**) specifically requires auditors to perform risk assessment procedures to evaluate the risks arising from the use of information technology (**IT**), design appropriate audit procedures in response to the identified risks, and communicate significant matters that support the preparation of the financial statements and related reporting requirements to management and those charged with governance.

During the 2024 inspections, the AFRC inspection teams noted incidences where the engagement teams lacked an understanding of the IT environments of their audit clients and perform an inadequate risk assessment regarding the use of IT by their audit clients. Consequently, they did not appropriately identify or assess the risks of material misstatement or design and perform sufficient further audit procedures. In such incidences:

1. Engagement teams lacked an understanding of the information systems used by their audit clients and did not appropriately assess the reliability of the data or records processed or generated by these systems relevant to the preparation of financial statements. For example, some engagement teams could only tell that an "accounting system" was used in the business process

but could not provide details, for instance, what accounting software had been used, whether any customisation had been made, and what system-generated reports had been used in the financial statement close process.

2. Engagement teams had a limited understanding of how the information flowed between systems. For example, during the audit of a retail client, the engagement team did not thoroughly understand how sales data was generated in the point-of-sale (**POS**) system and how such data was transmitted to the accounting system for bookkeeping purposes.

3. Engagement teams had minimal awareness of the cybersecurity environment in which their audit clients operate, in particular, businesses that use online platforms or are engaged in online trading. As a result, they failed to identify and assess cybersecurity risks and evaluate the measures and controls their audit clients have put in place to address such risks. In addition, the engagement team did not understand from their audit clients how cybersecurity incidents are managed and whether they have made sufficient provisions for system recovery costs, potential litigation costs, and compensation to stakeholders in case a cybersecurity incident occurs.

The AFRC inspection teams also noted that engagement teams relied solely on system-generated reports provided by third-party IT service providers, such as broker supplied systems (**BSS**) vendors, during the execution of audit procedures without assessing the completeness and accuracy of these reports.

Engagement teams are encouraged to promptly take action to understand their audit clients' IT environments for all their ongoing audit engagements if they have yet to do so. It could assist them in performing a proper risk-based and quality audit, and ensuring compliance with HKSA 315 (Revised 2019). To help auditors with this, we have included in **Appendix I**, a non-exhaustive list of matters that auditors may consider when getting to know the IT environments. Engagement teams are recommended to view our video, *AFRC Connect - Understand and Evaluate IT Risks and Controls*, which includes a case study to assist in understanding of the requirements. With that understanding, engagement teams will be able to assess the complexities of the IT environments, the risks

arising from the use of IT, and the need to understand and test general IT controls (**GITCs**).

When testing of GITCs is considered necessary, auditors may enlist IT audit service providers to conduct such procedures. These procedures may involve identifying, testing, and evaluating relevant GITCs and application controls, as well as performing substantive testing of IT process activities.

Appendix I

A non-exhaustive list of matters that engagement teams should consider when obtaining an understanding of the use of IT by their audit client: