External Auditor's Responsibility to consider Cybersecurity

September 2018

One of the most complex and rapidly evolving issues which affect all entities is cybersecurity. This leads to the question of whether cybersecurity risk is relevant to the audits of financial statements. What is the auditor's responsibility in respect of cybersecurity risk when planning and performing audits?

Scope of auditor's responsibility

The auditor is required to:

- Understand how the business uses IT and the impact of IT on the financial statements,
- Understand the extent of the company's automated controls as they relate to financial reporting (including IT general controls that are important to the effective operation of automated controls and the reliability of company-produced data and reports used in the audit), and
- Use his or her understanding of the business's IT systems and controls in assessing the risks of material misstatement of financial statements, including IT risks resulting from unauthorized access.

The immediate conclusion may be that cybersecurity risk is not an area that requires special audit attention, but auditors would consider, as part of the risk assessment process, an entity's business risks in the audit of financial statements. Cyber incidents can result in financial consequences and therefore, have an effect on the financial statements.

Cybersecurity risk should therefore be considered in every financial statement audit. Auditors should consider and assess the impact of such risk to the financial statements and, where necessary, the extent of the audit response required to address the risk.

It is important to note that the auditor's role is limited to the audit of the financial statements and does not encompass an evaluation of cybersecurity risks of the company's entire IT platform but only focusses on systems and controls affecting information used in the compilation of these financial statements.

Risk consideration and assessment

Risk assessment is part of the financial statements audit process and is a key fundamental process which must be performed during the planning phase of every audit. The auditor is required to identify and assess the risks of material misstatement in the financial statements, through understanding the entity and its environment, including the entity's internal control. With an in-depth understanding of the entity's business and environment (this includes an entity's IT and cyber environment), it enables the auditor to identify the risks, and to design and implement appropriate audit responses to address those identified risks. The auditor should obtain an understanding of the IT general controls, evaluate their design and determine whether the controls that are relevant to the audit have been implemented.

The auditor should determine whether any of the risks identified (which could include cyber-security risks) are, in the auditor's judgement, significant risks that require special audit consideration. If information about a material breach is identified, the auditor would need to consider the impact on financial reporting, including disclosures, and any reporting obligation.

Re-Assessing Cybersecurity Risk Every Year

Changes in the risk environment and the ways in which businesses operate mean that business risks do not remain constant. In one year, cybersecurity risk may not have been identified as a key business risk that may result in risks of material misstatement, but this does not mean that the same will apply for the next year. Significant and rapid changes in information systems, incorporation of new technologies into production processes, or expansion of operations can bring about new cybersecurity risk.

Audit responses to risks identified

Where cybersecurity risks may result in risks of material misstatement at the financial statement level, the auditor should take appropriate steps to address these risks. This may include assigning more experienced staff or those with special skills such as IT specialists to the engagement, incorporating additional elements of unpredictability in the selection of further audit procedures to be performed and modifying the nature of audit procedures to obtain more persuasive and corroborative audit evidence.

The auditor would have to determine whether continued reliance can be placed on the IT dependencies/automated controls; consider the need to revise the initial risk assessment, and the impact to the nature, timing and extent of other planned audit procedures. The auditor would have to respond to the ineffective IT control environment by obtaining more extensive audit evidence from substantive procedures.

Audit responses to cyber attacks

Companies that fall victim to successful cyber-attacks may incur substantial costs and suffer significant damage. The auditor should:

- Understand the nature and cause of the incident, carefully consider the costs and any adverse consequences arising from the cyber incident, and evaluate the impact it may have on the financial statements.
- Assess the impact of the attack on the entity's future revenue, potential litigation expenses, cybersecurity protection costs, etc and future cash flows, which may affect impairment assessments.
- Examine whether the breach may indicate going concern issues for the entity.
- Evaluate whether appropriate disclosures are included in the financial statements.
- Consider any other requirements to notify the appropriate authorities in case management has not made appropriate disclosures or considered the auditor's recommendations.