AUDITING WHAT IS EASY



DEVANESAN EVANSON

INTERNAL audit is intended to provide independent assurance, identify risks, evaluate controls and help organisations improve governance and performance.

Yet, despite having an internal audit function, many organisations continue to experience fraud, control failures, regulatory breaches, operational problems and strategic surprises.

The problem is often not whether an organisation has an internal audit function, but how that function is positioned, managed and carried out.

An internal audit function can fail even when it has competent auditors, because weaknesses in independence, risk assessment, communication, skills, culture and follow-up undermine its effectiveness.

Independence is fundamental to effective internal auditing. Internal auditors must be sufficiently independent from the activities they audit.

Problems arise when the chief audit executive reports primarily to management rather than having meaningful access to the audit committee or board. Auditors may then become reluctant to challenge senior executives or report sensitive findings.

An internal audit function that is afraid to tell management uncomfortable truths cannot provide effective assurance.

A common weakness is focusing on routine and low-risk areas rather than significant organisational risks.

Auditors may repeatedly audit expenses, procurement documentation or compliance checklists because these areas are familiar and relatively easy to audit.

Meanwhile, major risks involving strategy, cybersecurity, artificial intelligence, third-party relationships, financial reporting, business continuity, culture or management override may receive inadequate attention.

Effective internal audit should be risk-based, not merely activity-based.

POOR AUDIT PLANNING

Weak audit planning can cause internal audit resources to be directed toward the wrong priorities. An annual audit plan should be based on a proper understanding of the organisation's objectives, risk profile, emerging risks, regulatory environment and control weaknesses.

If the audit plan is simply rolled forward from previous years, internal audit may continue examining yesterday's risks while missing tomorrow's threats.

Compliance is important, but internal audits should not become merely a compliance-checking function.

An audit that confirms whether policies were followed without considering whether those policies and controls actually manage the underlying risks provides limited value.

For example, an auditor may confirm that procurement forms were properly completed without asking whether the organisation is obtaining value for money, whether suppliers are appropriately selected or whether conflicts of interest exist.

Internal audit should examine not only "Were the rules followed?" but also "Are the rules and controls achieving their intended objectives?"

WEAK UNDERSTANDING OF THE BUSINESS

Auditors who do not understand the organisation's business model may struggle to identify significant risks.

Understanding the business means knowing how the organisation makes money, delivers services, interacts with customers, depends on suppliers, uses technology and creates value.

Without business knowledge, auditors can become overly focused on transactions and documentation rather than understanding the bigger picture.

The risks facing organisations are becoming increasingly complex. Internal auditors may need knowledge of data analytics, cybersecurity, technology, financial reporting, fraud, risk management, sustainability, artificial intelligence and regulatory developments.

A traditional audit skill set may no longer be sufficient.

Internal audit fails when it continues using yesterday's methods to examine tomorrow's risks.

Continuous professional development is therefore essential.

Another major weakness is identifying symptoms rather than causes.

For example, an audit may report that several payments were made without proper approval. However, simply recommending that staff "comply with the approval procedure" does not address why the problem occurred.

The real cause might be inadequate system controls, unclear authority limits, unrealistic processing deadlines or management override.

Without identifying root causes, the same problem is likely to recur.

WEAK AUDIT REPORTS

A technically correct audit report can still fail if nobody understands why the findings matter.

Reports sometimes contain lengthy descriptions of procedures, excessive technical language and numerous minor findings while failing to explain the business impact.

A strong audit report should clearly communicate:

What happened? Why did it happen? What is the risk? Why does it matter? What needs to change? Who is responsible?

Senior management and the board need meaningful insights, not simply lists of control deficiencies.

Internal auditors must be willing to challenge assumptions.

If auditors accept management explanations without sufficient evidence, they may become overly dependent on management's perspective.

POOR FOLLOW-UP

An audit is not successful simply because a report has been issued.

If management agrees to corrective actions but nobody verifies implementation, findings can remain unresolved for years.

Effective follow-up should determine whether agreed actions were actually implemented and whether they have adequately reduced the underlying risk.

Repeated findings are often a sign that internal audit's recommendations or management's corrective actions are ineffective.

Internal audit performance is sometimes measured by the number of audits completed, reports issued or findings identified.

These measures can encourage auditors to focus on activity rather than impact.

A better question is whether internal audit has helped the organisation identify significant risks, strengthen controls, prevent losses and improve governance.

The writer is a former chief executive officer of Minority Shareholders Watch Group and has over two decades of experience in the Malaysian capital market.