ACCOUNTANCY IRELAND
APRIL 2015 VOL.47 NO.2

INTERNAL AUDIT PRIORITIES

For the majority of internal auditors, cyber security, risk management, outsourcing, social media and data protection are top concerns according to the results of a Deloitte survey conducted last year. Internal auditors must be able to adapt quickly to keep pace with changes in these areas but for those with the right skills, there are growing opportunities to contribute value across a wide range of organisations. **David Kinsella** explains.

A majority (75%) of heads of internal audit who responded to a survey conducted by Deloitte last year noted an increase in stakeholder expectations of the internal audit function. Among the key areas identified by respondents were:

- Cybersecurity;
- Risk and control;
- Outsourced activities;
- Social media activities; and
- Data Protection.

CYBERSECURITY

Cyber crime and cyber attacks across all industry sectors and both large and small entities are increasing more rapidly than the abilities of many organisations to detect, prevent and manage them. Cyber criminals are increasingly adept at gaining undetected access and maintaining a persistent, low-profile, long-term presence within information technology environments. Many organisations leave themselves vulnerable to cybercrime based on a false sense of security, perhaps even complacency and there is no shortage of evidence of lack of understanding of the evolving threats combined with use of non-agile security tools and outdated processes. Notwithstanding the potential significant reputational and financial impact of cyber crime it seems organisations are failing to recognise the threat in their IT environments and are misallocating limited resources to lesser threats.

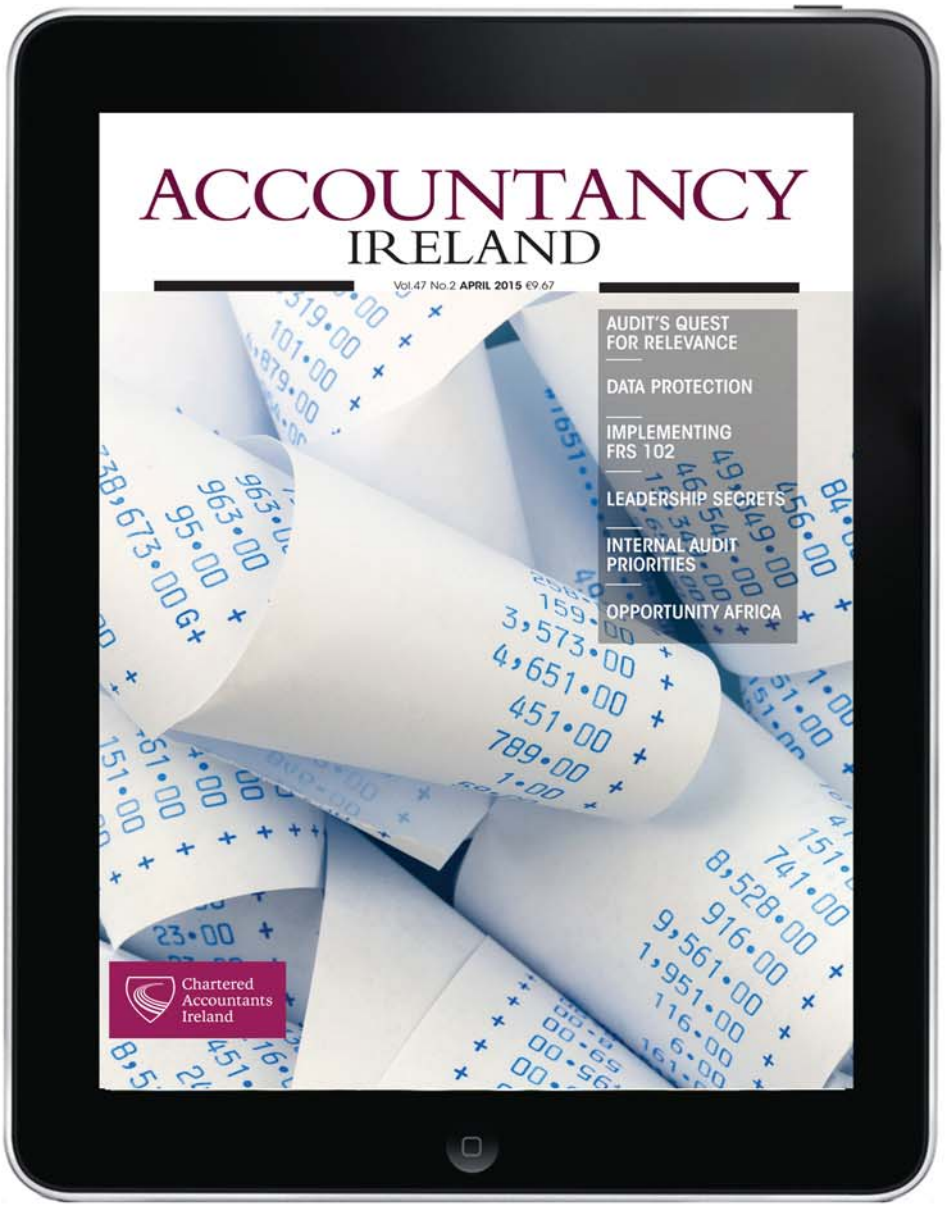
It is imperative that internal audit takes a leading role in determining whether an organisation has a systematic and disciplined approach to evaluate and strengthen the effectiveness of cyber risk management and determine whether appropriate cyber security capabilities (people, process, and technology) are in place to protect against cyber threats.

RISK AND CONTROL FRAMEWORKS

Shortcomings in risk and control culture continue to underlie many organisational failures. Indeed, an organisation's risk and control culture – the norms, attitudes, and behaviours related to risk awareness, risk taking, risk management and controls that shape decisions on risk – plays a major role in influencing the day-to-day decisions of management and employees and has a significant impact on the risks they assume.

Accordingly, regulators are adopting an increasingly sceptical approach in their engagement with boards and senior management on whether the organisation's risk and control culture supports adherence to the board-approved risk appetite, is appropriate for the scale, complexity, and nature of its business and is based on sound, articulated values carefully managed by the leadership of the organisation.

“NOTWITHSTANDING THE POTENTIAL SIGNIFICANT REPUTATIONAL AND FINANCIAL IMPACT OF CYBER CRIME IT SEEMS ORGANISATIONS ARE FAILING TO RECOGNISE THE THREAT IN THEIR IT ENVIRONMENTS AND ARE MISALLOCATING LIMITED RESOURCES TO LESSER THREATS.”



Get the full issue in your App store

Available on the App Store

GET IT ON Google play

As a result, boards and senior management are considering ways to foster a stronger risk and control culture within their organisations. Internal audit has a key role to play and should develop a culture assessment framework and execute internal audit activities to assess whether the prevailing risk and control culture, and related processes, actions, and 'tone at the top' align with the organisation's values, ethics, risk strategy, appetite, tolerance, and approach.

Organisations that have adopted COSO[1] may wish to consider implementation and embedding of the COSO 2013 Framework which became effective in 2014. Under this framework, companies are required to assess whether the 17 principles (*Figure 1*) underpinning the framework are 'present and functioning' in determining whether their system of internal controls is effective.

OUTSOURCE PROVIDERS / EXTENDED ENTERPRISE

The use by organisations of third-party service providers presents additional control risks. Historically, internal auditors sought to determine that the business and management retained ultimate responsibility for outsourced services and to assess the management of outsource providers by examining contract compliance, performance monitoring, and governance. Recently, the focus has shifted to include more specific risks such as contingency strategies and data protection. Questions to consider include:

- What do we do if the service provider can no longer support us, in particular in the context of an unplanned scenario?
- Has the business considered circumstances in which services might be lost unexpectedly?
- Has the business identified potential alternative providers?
- In an emergency situation, how would the transition to a new provider in an emergency take place? What data would these providers have access to and how would they protect it?
- Does the third party have controls at least equivalent to those in your own organisation?
- Do you understand what data the third party has and how they retain and manage it?

> "WHILE THE BENEFITS ARE CLEAR THERE ARE ALSO SIGNIFICANT RISKS TO CONSIDER SUCH AS INFORMATION LEAKAGE, SOCIAL ACCOUNT HACKING AND PEOPLE CONCERNS."

SOCIAL MEDIA

Social media has evolved to become an integral part of the business landscape. While the benefits are clear there are also significant risks to consider such as information leakage, social account hacking and people concerns. Internal audit has a role in assessing the organisation's overall social media governance policy. Areas of focus might

include monitoring the organisation's social media presence, incident response processes, alignment of social media activity to the organisation's overall strategy, content approval controls and third party contract management arrangements where third party vendors are used to support the social media agenda.

DATA PROTECTION

Growing numbers of organisations have suffered loss or leakage of their data through unlawful acts or by way of human error. Internal auditors have a role in assessing organisational controls aimed at mitigating potential data loss such as restrictions on the use of physical media, mobile device security, and network monitoring. One of the biggest issues many organisations face is failure to understand the type and extent of data that they hold. Consequently, internal auditors should assess:

- whether the business knows what data it holds;
- where the business knows where that data is held; and
- if whether the organisation's data retention policies are adhered to.

ADAPTING TO STAY RELEVANT

It is critical that internal auditors continually self-assess to ensure that their approaches are effective and insightful. Internal audit teams require both experience and professional standing to challenge the business and question the status quo, particularly in areas where professional judgement is required such as change, culture, risk and governance. Specialists may be required to provide rigorous challenge in some of the areas under review.

Continued improvements in how internal auditors conduct their work are necessary in order to keep pace with change. The use of data analytics, for example, still in its infancy is an area where internal auditors will need to develop expertise.

Engagement with broader stakeholder groups and increased expectations are here to stay. Internal auditors need to embrace this and seek ways to actively interact with stakeholders to demonstrate the full potential of internal audit.

This is an exciting time with growing opportunities for internal auditors to add insight and value to their organisations. I hope that you find this article useful in identifying some of those opportunities.

Figure 1: 17 Principles underpinning the COSO Internal Control Framework

Control environment

1. Demonstrates commitment to integrity and ethical values
2. Exercises oversight responsibility
3. Establishes structure, authority and responsibility
4. Demonstrates commitment to competence
5. Enforces accountability

Risk assessment

6. Specifies suitable objectives
7. Identifies and analyzes risk
8. Assesses fraud risk
9. Identifies and analyzes significant change

Control activities

10. Selects and develops control activities
11. Selects and develops general controls over technology
12. Deploys through policies and procedures

Information and communication

13. Uses relevant information
14. Communicates internally
15. Communicates externally

Monitoring activities

16. Conducts ongoing and/or separate evaluations
17. Evaluates and communicates deficiencies

Source: coso.org May 14, 2013.

David Kinsella, FCA is a Partner in Deloitte's dedicated Enterprise Risk Services department and specialises in the provision of internal and risk advisory services.

Notes:

1 COSO – the US Committee of Sponsoring Organizations of the Treadway Commission. COSO – supported by five organizations: Institute of Management Accountants (IMA), the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), the Institute of Internal Auditors (IIA), and Financial Executives International (FEI).