Deloitte.

Directors' Series
BEYOND COMPLIANCE

Succeeding amid change and uncertainty: Action plans for audit committees

Riding the technology wave

Gone are the days when technology was the IT department's responsibility and an organization's technology was fully contained within its own walls and used exclusively for work-related activities.

Today, almost every activity is technology-enabled in some way. The lines separating technologies for personal use and work purposes have been erased as employees use work computers for personal tasks while conducting business activities via their personal devices.

With technology now an integral part of almost every activity and project, audit committees are responsible for more than just monitoring budgets and the deployment of technologies. They should also see that appropriate controls are in place to ensure the security of data and the confidentiality of private information. These controls may include education programs, traditional password, firewall and antivirus practices, and monitoring and surveillance practices.

Bring Your Own Device (BYOD)

BYOD – Bring Your Own Device – reflects a world where employers expect to reach employees anytime, while employees need to take that call from anywhere. BYOD offers organizations opportunities for lower procurement costs, increased efficiency and heightened employee commitment. But it also requires organizations to assume technology support for their employees' devices along with material maintenance, the need to ensure compatibility, training and employee expense reimbursement.

Cloud

Cloud technologies make data accessibility possible from almost anywhere, enabling employees to work from any location. However, when the organization's data is accessible from any location, protecting it is of primary importance. Robust data protection programs must be implemented – by the organization and its third party providers – including reliable backup, recovery plans, passwords, firewalls and cyber security.

Shared services

Outsourcing is an efficient, cost-effective way to access an extended talent pool to perform various non-core activities. Although these activities are performed outside the organization, management remains responsible for them. Audit committees should ensure that proper controls have been put in place to protect the information used by the outsource provider and ensure the reliability of information that provider creates for the organization. Since the organization continues to own the data, protective programs are needed to recover data, transfer the service to another supplier or take the service back in-house if problems arise.

Social media

Organizations are using social media to build relationships with customers and other key stakeholders, while increasing their own efficiency and effectiveness.

For example, organizations no longer need to maintain subscription services, which is a time and resource consuming exercise. Instead, many now allow subscribers to login using their social media profiles, an approach similar to outsourcing customer relationship management to a third party, which eliminates the need for the organization to maintain contact information or dedicated mailing platforms.

Audit committee action plan…

- Ensure IT strategy is aligned with the organization's overall business strategy.
- Understand and manage the organization's technology risks including cybersecurity.
- Regularly review IT policies to ensure they take into account emerging technology.
- Ensure that an education program is in place to stay abreast of evolving technology developments.

Activities that capture and utilize subscriber information need controls to protect that information from improper use. Organizations also need a recovery plan so they can continue reaching their subscribers if problems arise with the social media service.

Cyber threats

No organization should underestimate the cyber-related threats it faces, either directly or through its relationships with others.

Cyber threats are actually a new form of old risks. Similarly, the risk management steps taken for physical properties need to be adapted to virtual facilities. These include access rights, recovery plans, background checks, ensuring that a competent team is in place, education programs to build employee skills, and more. New tools are also being developed to help mitigate cyber threat risks. Similar to the way antivirus applications are developed, these tools collect knowledge around cyber attacks provided by participating organizations, and use data analytics to detect indicators of potential threats in order to deploy appropriate defense strategies.

Data analytics

All technology approaches involve collecting data for a variety of purposes: procurement, invoicing, subscriptions, recruiting, and so on. With the advent of cheaper, powerful technologies, organizations of all sizes can cross tabulate the information they collect to create intelligence from raw data.

Data analytics is a powerful tool to help management make informed decisions, though some important issues need to be managed:

- **Privacy and confidentiality.** Organizations often collect data for a specific purpose, such as a subscription. However, they should not use that data for other purposes – such as to identify opportunities to sell additional services – without the legal and social right to do so.
- **Expertise.** Data analytics – digging for filtered information in various databases – requires knowledgeable experts to assess all of the data variables and turn that information into useful intelligence.

Audit committees should ensure that the right protections are put in place to maintain the integrity of data analytic activities. These include employee education programs, instituting a privacy policy and confidentiality agreements to govern the appropriate use and dissemination of data, rights of access to captured data and obtaining express consent from individuals who have provided confidential information.

The IT department

While the IT department is no longer solely responsible for an organization's technology, it still plays a central and increasingly important role as technology use continues to expand. A continuous learning program should be implemented to keep the IT team members current with emerging technologies so they can support the organization and be a strategic advisor to senior management and the board of directors.

To download the full report or connect with one of our Deloitte experts, please click here: www.deloitte.com/ca/successfulauditcommittees.