Chartered Institute of Internal Auditors / Audit Leaders

Digital media and the role of internal audit

In relative terms, digital media is still a new concept and the pace of innovation has resulted in capabilities being made available at a rate that is faster than organisations have traditionally been able to adapt to. Organisations and the individuals within them may not be afforded the luxury of time to adapt as new technologies bring immediate transformation. Understanding the impact of digital media in the overall control environment is a prerequisite for internal audit in the 21st century.

Who are the stakeholders?

The board

The board is most likely to take a strategic approach seeking assurance as to the digital capability of the organisation. However, other functions also have a keen interest in this subject.

Marketing

Marketing colleagues specifically think of advertising in respect of digital media. They would expect a digital media audit to provide assurance over their processes and the effectiveness of techniques being used to measure campaign success.

Technology

Technology colleagues would generally be concerned with media storage and access including security, data owner accountability, software support, rather than the data itself.

Legal/governance

Legal/governance colleagues are generally concerned with the protection of corporate interests such as litigation, copyright and other intellectual property issues.

Why should this be an audit consideration?

From central government, local council, retail, manufacturing, healthcare, utilities and financial services, it is difficult to imagine that digital media does not form a part of the data set. The extent to which it is material however will vary from organisation to organisation. Chief audit executives (CAEs) need to think ahead as to the planned or potential digital journey for the business and the associated risks.

The organisational benefits of collaboration tools for communication (eg Microsoft Teams, WhatsApp, and Messenger) and efficiency (eg virtual meetings such as Zoom) also enable employees to inappropriately share data. In some instances this may also extend to granting third parties access to systems requiring new approaches to data security controls and/or a higher appetite for risk.

For CAEs there are always difficult decisions as to which assurance needs to fulfil with finite resource. Consideration of the risk profile must always be the first priority, although it is hard to imagine any sector unaffected by the digital revolution and so understanding ones digital capability and the associated risks should ideally be factored into the audit plan.

Audit thoughts for the plan

Before getting into the detail of specific audits, the institute recognises that 'digital' is a relatively new concept for some internal audit functions and their organisations. It may be that there are skill gaps which need development or that these audits, while beneficial cannot be prioritised over more pressing assurance needs. CAEs may wish to give consideration to outsourcing some of the audits detailed below. This may also add value through access to benchmarking data and alternative approaches.

Digital capability audit

Also referred to as digital readiness, this type of audit gives an indication as to competence and whilst it may not be necessary to be advanced in all digital aspects, an organisation should be at least as proficient as its peers.

It should include assessment of skills and evidence of strategy in relation to online presence, digital marketing, customer interaction, supplier interaction, mobility of services, information security, data management, technology and organisational strategy. Findings could position the entity as novice, developing or advanced in each area identifying associated risk exposures and opportunities.

Risk considerations:

- Unauthorised data sharing particularly with collaboration tools.
- Alignment of digital skills capability with business strategy.
- Impact of end user capabilities on the effectiveness of control frameworks.
- Digital disruption.

Digital advertising media audit

Online advertising is achieved through paid, earned (consumer advocacy, word of mouth, sharing) and owned (corporate websites, Twitter/Facebook accounts, blogs) advertising.

Paid advertising typically starts with defining the advertising objective, identifying the target audience, researching where they are active and the type of media that resonates with them (audio, video, text). Does it comply with advertising standards? The performance of the advertising campaign is then tracked. Is it reaching its audience? Has it generated engagement? Is text getting enough clicks? Is creative attractive enough? Adaption may be required. After the campaign, analysis should be undertaken as to establish if the objective was met and to inform future marketing activities.

Common forms of digital advertising:

- Social: using channels such as Facebook, Twitter, Instagram.

- Display network: the type of ads that are seen on the sidebar of internet searches.
- Search engine: paying to be at the top of search engine results.
- Mobile: banners and videos that pop-up on mobile devices in apps and searches.
- Video: common on YouTube and free apps, requiring users to watch a video before their chosen content.

Risk considerations:

- Repeatability of unprofitable campaigns.
- Identification of new media options.
- Ethical use of algorithms to curate content.
- Breach of regulatory obligation ie Advertising Standards Authority (ASA) rules.

Digital content audit

This type of audit can be likened to asset management…but on a bigger, less tangible scale. All data should have a defined data owner, with accountability for its management. It is not acceptable for business to assume that the IT department does this – would a house builder be expected to maintain the décor and contents of a house after the keys have been handed over?

A content audit could establish and provide assurance over the processes for ensuring that data is maintained to be valid, accurate, complete, reliable, timely and relevant. Even small organisations accumulate vast quantities of digital data and it may be advisable to audit by data type, data owner or another appropriate classification to keep the scope manageable. There are digital asset management tools (software) to efficiently store, organise, find, retrieve and share digital files.

Significant focus is placed on personal data due to the General Data Protection Regulation (GDPR). However, this should not detract from the effective management of all data, particularly digital where almost infinite storage and retention is possible.

Risk considerations:

- Data storage capacity/capability, cost and obsolescence.
- Security breaches and near misses.
- Data retention ie no longer than is necessary for the purpose intended.
- Location of data storage eg UK, EU or worldwide - particularly cloud, outsourced, third party and customer data. Volume limit of current tools for effective control of data.

Digital media protection - technical

All digital media is electronic and therefore this could essentially be a data security audit with the scope perhaps targeted to specific digital data sets. It may however be appropriate to differentiate the scope by focusing on the media itself rather than the systems, such as that which is critical to the organisation, created internally or shared with partner organisations.

Risk considerations:

- Securing files by default.
- Controlling files by design.
- Innovation practices.

Digital media protection - legal

The exponential volumes of data being created, 'big data', is revolutionising the way digital data is being created, collected, communicated and used. Clarity over the source and legal ownership of data is important to avoid litigation. Corporate/competitive advantage may be reliant on algorithms used to understand data; safeguarded by internal control mechanisms as outside of intellectual property rights. Additionally, for digital media that is also personal, the introduction of the GDPR has the potential to create a more litigious society than previously experienced in the UK.

Risk considerations:

- Human error or intention causes reputational damage/litigation.
- Infringement of intellectual property rights.
- Negative attention/defamation as a result of interaction on social media platforms, review sites etc.

Resale of digital content products

The Consumer Rights Act 2015 covers the rights of consumers buying digital media, distinct from products and services, examples of which include computer system software, films, games, books, downloaded music and mobile phone application software (an app). The act also defines requirements where digital content forms only part of a product; ‘mixed contract’.

Where organisations resale digital content it would be prudent to audit the associated processes to ensure that the act is complied with, particularly where faults are identified.

Risk considerations:

- New product/service risk impact assessment.
- Maintaining authenticity of product.
- Innovation practices.

Closing thoughts

The word *digital* sees no boundaries between sectors as it permeates through the most traditional of organisations. Unless using paper and quill based systems, these topics are relevant to all functions - every organisation with a website is undertaking some form of digital advertising even if it is a simple awareness campaign. The risks are here, the threats and opportunities that come with digital media - are the audit plans and auditor skills aligned to them?

> *"Facts do not cease to exist because they are ignored"*

- Aldous Huxley

Further reading

Consumer Rights Act 2015

Advertising Standards Authority (ASA) codes

General Data Protection Regulation (GDPR)