GDPR - the expansive role of internal audit

In an era of big data and digitalisation, the financial and reputational penalties from a data breach mean that the General Data Protection Regulations (GDPR) will always be high profile. Audit leaders need to maintain proportionality; it would be remiss to continue to advise on improving data management processes when an organisation is heading into liquidation. A major data breach could, likewise, be disastrous if everyone, including internal audit continues to focus on an aggressive acquisition strategy.

On 25th May 2018, with a fanfare rarely seen in the compliance world, GDPR came into force in the UK. This guidance briefly summarises it and encourages audit leaders to think about a broad spectrum of compliance assurance for the internal audit plan.

Post-Brexit

An almost compulsory prelude to any discussion…

The Data Protection Act 2018 will remain in place. The government intends to bring GDPR directly into UK law on exit as part of the EU Withdrawal Bill, with minor adjustments in respect to law and enforcement arrangements.

The Information Commissioners Office (ICO) has guidance on this.

The government has published details of amendments in the event of a no-deal Brexit.

GDPR summary

GDPR specifically relates to personal data.

At its heart are seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

When it became law, the ICO noted that GDPR represents an 'ongoing journey' and this is how organisations should be thinking about compliance with the rules.

At the time, the information commissioner, Elizabeth Denham said “those that merely comply, that treat the GDPR as another box-ticking exercise, miss the point. And they miss a trick because this is about restoring trust and confidence. This is about commitment over compliance. It is up to you and your boards, and your leadership teams to foster a culture of transparency and accountability as to how you use personal data.”

The role of internal audit

GDPR legislation stipulates that organisations should have procedures in place for regular testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of data processing.

Internal auditors across the country completed GDPR readiness reviews; it was THE hot topic from 2016 through to implementation in May 2018!

What now though? How does GDPR feature on the audit plan now it is competing with other risks?

We look at four areas for audit leaders to consider: data governance, third party management, cyber-security and compliance.

Data governance

As organisations continue their digital transformations, higher and higher volumes of data are stored and processed, which intensifies the criticality of data governance. GDPR compounds this further. As with culture, the tone at the top is an important factor in GDPR.

The scope of a data governance audit could provide assurance relating to questions such as:

- Does the board take accountability for data, both collectively and as a named individual – where does the buck stop?
- Is there evidence of a robust approach to identify and assess data risks?
- Has the board defined its risk appetite for data security and regulatory compliance?
- Does governance facilitate proactive rather than reactive management of data?
- Can a data privacy culture be evidenced?
- Are data policies and processes appropriate for the organisation?
- Is the strategy towards and management of big data proportionate for the activities of the organisation?
- Could the strategic aims of the organisation put pressure on existing governance arrangements?
- Is there clear responsibility for GDPR compliance within the second line of defence?

This is an extensive topic and this list is by no means comprehensive.

Audit leaders will want to reflect the maturity of their governance arrangements when scoping the audit. It may be that a consultancy approach is an appropriate first step or a targeted piece of assurance on data strategy rather than go straight into data governance. Each organisation will be at a different place on their commitment and compliance journey.

Auditors should not restrict their governance work to personal data. In May 2019, the EU introduced the Regulation on the free flow of non-personal data. All data is regulated.

Governance is one aspect of a data framework. A 2019 presentation on data governance to the IIA chapter in Seattle by Protiviti is a useful reference point for audit leaders thinking about this area.

Third parties

When we consider the complexity of systems and use of cloud services, third parties feature in the data flow for most organisations.

If your organisation is the data controller and uses a third party for data processing, liability in the event of a breach is not automatically transferred. The ICO has clear guidance on this. Any audit of third party management must include GDPR.

Specifically, assurance may be considered as to how contracts and terms take GDPR compliance into account. What revisions to due diligence have been made? Do risk assessments sufficiently address data exposures? Is GDPR compliance verified where volume/sensitivity of data is material?

Most importantly how does the organisation ensure that no third parties sub-contract data management?

Cybersecurity

Article 5 of the GDPR requires personal data to be processed in a manner that ensures the appropriate security of such data, including protection against the risk of destruction, loss, alteration, and unauthorized disclosure or access.

Whilst cyber has been a regular feature on audit plans for many years, some commentators believe that GDPR has heightened the risk profile for many organisations. Is this true of your organisation?

Outsourcing IT to the cloud shows no signs of abating and the same security misconfigurations that are made internally are now being made in the cloud. While public cloud providers must be vigilant in how they protect their data centres and apps, responsibility for securing access to those services lies with organisations themselves.

In 2020, however, the emphasis of Risk in Focus is on the need for internal audit to step up to meet the assurance demands of organisations. Co-sourcing and outsourcing IT security audits is a valuable means for acquiring know-how, especially ethical hacking expertise. However, relying solely on third-party assurance is not enough.

Given the financial and reputational costs of cyber breaches and data leaks, chief audit executives have a strong case to make with their boards and audit committees for increased budget allocations to address this interminable risk.

Internal audit must also be cognisant of the new reality that data privacy and protection principles need to be

embedded into cybersecurity controls.

Risk-based security programmes provide a framework for the prioritisation of threats enabling organisations to invest in controls for maximum benefit. How does your organisation determine its cyber priorities?

A major change as a result of GDPR was to give individuals ownership of their data. This introduced two new risks to data security which auditors should be aware of.

Firstly, hackers can use right of access requests to obtain data that the company holds on individuals. This is particularly useful in identity theft and targeted phishing campaigns where the hack has been undetected. What controls exist to be sure that data is being released to the right person?

Secondly, organisations must be able to provide an individual with their digital footprint - the data held on them. Data portability opens communication channels that would previously not have existed. How is this data presented and transmitted? Is it encrypted? Members of the public may have limited security awareness; how can organisations protect themselves from subsequent data misuse?

Questions for internal audit to ask their organisations regarding cybersecurity:

- What evidence is there that the organisation has got the basics covered? These basics include malware detection, regular software updates, staff awareness training and access rights management.
- Is the organisation aware of the changing profile of its cyber risks given the changing nature of its operations, particularly as the company digitalises?
- Is the IT security function staying up to date with evolving information security threats?
- Does internal audit need to add staff and expertise in order to bolster its cyber/information security capabilities? Is the function over-reliant on third party service providers for cyber risk assurance?
- Does the internal audit function verify that penetration testing by the second line of defence is robust and comprehensive, including reperformance to obtain evidence of that?
- Additionally, is the third line of defence expected to provide independent hacking, in addition to reperforming first- and second-line pen testing? Is it doing this?
- To what extent is the organisation compliant with GDPR? What progress has been made in the last 12 months? Is the business fully aware of the company's obligations under GDPR and are the IT security function and the compliance function familiar with the security aspects of GDPR?

GDPR Compliance

As the third line of defence, internal audit is not responsible for checking that an organisation is complying with specific GDPR requirements. It is the responsibility of the first and second lines. However, in small or evolving organisations where there is limited second line activity, audit leaders may be required to carry out such compliance checks.

Audit leaders should understand what GDPR assurance looks like for their organisation. Ideally, documenting this in an assurance map assists not only internal audit planning but the audit committee too in navigating the associated complexities.

Most organisations will have a nominated Data Protection Officer whose responsibilities include GDPR compliance.

Important questions to consider in this regard include:

- Is the DPO's approach proactive or reactive?
- Is the DPO appropriately trained and staying up to date?
- Does the DPO report directly to the CEO to provide a degree of independence from the organisation?
- Does the DPO have a budget to seek external legal advice if and when necessary?
- Has consideration been given to the DPO providing a report to the audit committee and attending annually to provide an update to the audit committee regarding the organisation's compliance with GDPR?
- Have data flows and inventory been maintained since the GDPR implementation project?
- How does the DPO ensure data protection is by default and design?
- What risk methodology does the DPO use?
- How does this fit into the wider risk approach by the organisation?
- Are data policies/procedures fit for purpose and maintained?
- Does the programme of work for GDPR (and the DPO) tie up with the risk profile?
- What role does the DPO have in the induction of new employees?
- What monitoring controls do they rely on?

This is a sample of the many questions internal audit can evidence to provide assurance over GDPR compliance. Technical guidance on compliance is also available.

Competing priorities

With limited budgets and increasing organisational complexities, many audit leaders find themselves with growing assurance gaps. The high profile of the GDPR and its potential fine of 4% of global turnover or €20 million whichever is the greater, make it a priority for audit committees. But should it be?

A risk-based audit plan will ensure that the GDPR's representation is appropriate and proportionate. Not only is this best practice but using and explaining this approach can be beneficial for audit leaders when their audit committee has a tendency to be reactive to hot topics or pressures experienced in other organisations.

GDPR non-compliance is one of many risks that could bring down an organisation…at an inherent level. From an assurance perspective however, the real concern is about residual risk. Which risks are not being or cannot be managed to an acceptable level?

Internal audit priorities specifically for GDPR must also include cyber which is fundamental to preventing data breaches. There will also be operational processes with intrinsic links to GDPR compliance, unique to each organisation's depending on its purpose. Potentially engagement planning for all internal audits should assess relevance to GDPR to build towards an overall opinion on compliance.

What next?

Audit leaders may wish to look ahead at preparations for other data regulations on the horizon.

California Consumer Privacy Act

Similar to GDPR and taking effect on 1 January 2020. It is regarded as the forerunner for legislation that will

be copied across other states in due course.

Any profit-making business with customers or employees in California is liable if it meets one of the following criteria:

- Has a gross annual revenue totalling over $25 million
- Holds the data of more than 50,000 California residents
- Derives more than half of annual revenues from selling California residents' personal data.

ePrivacy Regulation

This will replace the EU's existing ePrivacy and Electronic Communications Directive 2002. The revision is intended to support the digital economy although debate continues among EU member states as to the approach.

It is unlikely the text of the new regulation will be agreed before 2020. This is one to watch not only in terms of the content itself but the timing and applicability to the UK post-Brexit.

Closing Thoughts

The persistence of cyber threats, in addition to the financial and reputational costs associated with periods of prolonged downtime, stolen data assets and negative press coverage requires that internal audit remains vigilant and attentive. Even if a business's efforts to mitigate information security risk are highly mature, there is a need for the third line of defence to track these efforts, assess the ongoing evolution of the organisation's perimeter wall and stay on top of organisational and operational changes that impact upon the business's information security risk profile...and GDPR compliance.

Expectations of internal audit are increasing, and internal audit must rise to this challenge by improving its skills, capabilities and understanding of the threat.

"Data is a precious thing that will last longer than the systems themselves"

Jim Berners-Lee, inventor of the world wide web