Insurance internal audit

Market perspectives

Minds made for protecting financial services
When the financial services industry works well, it creates growth, prosperity and peace of mind for hundreds of millions of people. No other industry touches so many lives or shapes so many futures.

At EY Financial Services, we share a single focus – to build a better financial services industry, not just for now but also for the future.

We train and nurture our inclusive teams to develop minds that can transform, shape and innovate financial services. Our professionals come together from different backgrounds and walks of life to apply their skills and insights to ask better questions. It’s these better questions that lead to better answers, benefiting our clients, their clients and the wider community. Our minds are made to build a better financial services industry. It’s how we play our part in building a better working world.

ey.com/fsminds
EY continually gathers valuable insights into the challenges facing the insurance industry. In these briefings, we explain the role internal audit can play in helping organisations respond to those challenges.

Carrying out discussions across the insurance industry, looking at internal audit practices across multiple sectors and interacting with regulators have helped us identify five hot topics that internal audit needs to focus on: operational resilience, senior managers and certification regime (SM&CR), investment strategy, workforce-based regulations, and cloud security assurance.

Each of these areas brings its own challenges, and the expectations on internal audit in providing ongoing assurance is increasing. The failure to identify and address risks associated with SM&CR, workforce-based regulations, cloud security assurance and operational resilience could lead to fines and other regulatory action, as well as the potential for reputational damage. Continued financial market instability will put stress on the investment and capital positions of nonlife or general insurers (GIs). This will make decisions about investment allocation all the more important.

This briefing document aims to help you guide your future internal audit activity, inform the scope of items reviewed, increase the value internal audit brings to key stakeholders and aid the understanding of common challenges across the industry.
Operational resilience

Background
The operational resilience of financial services firms continues to be an area of focus of the Financial Conduct Authority (FCA) after featuring as a cross-sector priority in its Business Plan 2018/19. The Prudential Regulation Authority (PRA) and the FCA launched the joint discussion paper Building the UK financial sector’s operational resilience in July 2018. As described in EY’s response to the paper, ‘whilst this is a discussion paper, it would be reasonable to expect that, to a large extent, it outlines the key tenets which the UK regulators expect firms to adopt in the periods ahead.’

Operational resilience is the ability of an organisation to prevent, respond to, recover and learn from operational disruptions to survive and prosper. It also considers the firm’s ability to not cause harm to customers and the wider market during such events. Firms have historically focused on the resilience of specific systems rather than considering the resilience of an end-to-end business process. The ability to identify, resist and react to disruptive events, whilst adapting and reshaping operations in environments, is key for the firms’ ongoing success.

A firm’s resilience depends on its governance, corporate structure, controls and regulatory framework. Effective boards and the senior management must agree clear standards to be met. The regulators expect them to prioritise business services, which, if disrupted, have the potential to threaten the firm’s ongoing viability, cause harm to consumers and the market or undermine financial stability. EY’s operational resilience framework is explained in the figure below:
Key challenges

Operational resilience is not a new topic and firms are likely to already have a number of the components in place, including business continuity planning (BCP), disaster recovery and crisis management. Speaking to clients has helped us identify the following key challenges in achieving strong operational resilience framework:

- Establishing clearly the accountability and responsibility of senior managers (SMs) for operational resilience clearly
- Evidencing a customer- and market-driven approach to the prioritisation of key business services, and establishing an internal- and external-facing approach to defining impact tolerances
- Determining and implementing metrics to monitoring for operational disruption, and supporting enhanced decision-making at executive levels
- Anticipating and preparing for risks to resilience across the ecosystem that firms operate in
- Building operational resilience in the culture of the organisation; and adopting a ‘resilience-by-design’ mindset on how the firm designs and operates its strategies, processes and technologies
- Reviewing current talent strategies to ensure access to employees with the necessary resilience skills and experience
What could the scopes of internal audit include?

The scopes of internal audit will include the following:

**Governance:**
- Responsibilities and accountabilities for the senior management, including the board, the executive committee and key business services
- Oversight and monitoring, including:
  - The identification and understanding of the firms’ reliance on critical service providers
  - The prioritisation of work on operational resilience

**Process:**
- The setting, monitoring and testing of operational risk appetite and impact tolerances for disruptions to key business services, including the consideration of the implications of their interconnectedness with other financial institutions
- The identification and management of key business risks
- The mapping of systems, people and processes that support the organisations’ business services, including internal and external connections and dependencies
- Identity and access management
- The defining of stability KPIs and monitoring, including the implementation in third-party contracts
- Patch management, including the update of new systems and the patching of known vulnerabilities
- Ongoing resilience, continuity planning and testing, including:
  - The development and periodic reviews of the business continuity and disaster recovery, crisis management, and IT disaster recovery plans, including the development of alternative business procedures
  - The operational testing of the plans and action plan follow-ups
  - Scenario planning and stress testing of resilience and continuity
  - Staff training and awareness of business continuity, crisis management and IT disaster recovery requirements
  - The consideration of business continuity elements during the initial third-party suppliers’ onboarding process
  - Ongoing management and review of third-party BCP
  - Internal and external communications plans in the event of an operational disruption
### Background

The Parliamentary Commission on Banking Standards, formed by the UK Government following the banking crisis, published its report *Changing banking for good* in June 2013. There was a perception that ‘individuals in the industry had been rewarded for inappropriate behaviour and that enforcement action against individuals had been very rare.’

As a result, three interlinking regimes – SM, certification and conduct rules – were introduced, with the deadline for implementation for all FCA solo-regulated firms, including wealth and asset managers, on 9 December 2019.

### The SM regime (SMR)

All senior individuals who perform senior management functions (SMFs) within their firms will need the preapproval of the PRA or the FCA prior to taking up their roles. Each individual must complete a ‘statement of responsibilities’ (SoRs) clearly setting out the role being undertaken, which will be subject to the ‘duty of responsibility’ requiring SMs to take reasonable steps to prevent regulatory breaches in the area of their responsibility.

### The certification regime (CR)

The CR requires firms to annually certify the fitness and propriety of certain key employees who are not designated preapproved SMFs but are performing a role that could cause ‘significant harm’ to consumers, markets or the firms themselves.

### Conduct rules

There are now two tiers of conduct rules. Tier one outlines the conduct rules that all employees (excluding ancillary staff) must comply with; tier two outlines the conduct rules that those in SMFs must comply with.

The impact of the regimes described above is summarised in the diagram below:
Key challenges for insurers

All elements of the business operating model are impacted by the implementation of SM&CR.
There are a number of key operational matters that firms must consider in support of ongoing SM&CR compliance, which are:

- The allocation of ownership for SM&CR operations – Given the breadth of operational activities impacted by SM&CR, the roles and responsibilities need to be clearly documented, covering all impacted functions and processes.
- Assess fitness and propriety – The assessment of fitness and propriety for SMFs, certified individuals and non-SMFs is an ongoing requirement. Firms need to ensure that they are provided with a comprehensive view of the individuals’ suitability for their proposed functions.
- Population management and change management – Firms are required to develop processes that highlight changes to their SMFs and certified populations, as well as changes to the allocation of roles and responsibilities. Certificates need to be accurate at all times. Hence, the processes need to support real-time maintenance.
- Conduct training and breach monitoring – Firms must ensure that they provide all in-scope employees information regarding the conduct rules and specifically on how they relate to the roles they perform. In addition, firms must design and embed processes that facilitate the identification, management and escalation of any potential conduct breaches, as well as reporting processes, which ensure that the regulator is informed within the timescales mandated by the Financial Services and Markets Act 2000.
- Compliance with all SM&CR rules – It is vital to focus on the listing of all the rules that need to be met to deliver SM&CR compliance. Rules are spread across a number of documents (e.g., senior management arrangements, systems and controls, fit and proper test, consumer credit sourcebook and consultation paper), which makes this challenging but critical. Businesses should consider developing a thorough traceability matrix that provides a clear audit trail – from regulation through to the development of minimum standards and business requirements.

### Potential scope

Internal audit should consider the following areas within the scope of a review:

- **Review of documentation:**
  - SoRs and the firm’s management responsibility map
  - Governing committee’s terms of reference
  - High-level review of board and executive committee papers
  - The firm’s SM&CR policy and the details of supporting arrangements, including the hand over policy, and SMF change management procedures and controls
  - The reasonable steps framework and arrangements in place
- **Certification:**
  - Review of documentation:
    - Governance artefacts underpinning initial implementation, including regulatory interpretations and the initial identification of the certified population
    - Policies and procedures related to the certification, including the fitness and propriety (F&P) assessment, and procedures for monitoring changes in the certified population
    - A sample of the issued certificates, together with the supporting F&P assessment, comprising:
      - Existing colleagues (at regime inception)
      - New colleagues (since regime inception)
      - Colleagues that have changed roles
Internal audit should also consider the following approaches to delivering the review:

- **Scenario workshop:**
  - The facilitation of scenario workshops ensuring that SMF attendees consider the scenario from a practical perspective
  - Assessment of the extent to which workshop attendees give consideration to the duty of responsibility and the evidencing of reasonable steps
  - Maintenance of a log of reasonable steps evidence referenced by SMFs throughout the workshop
- **Post-workshop testing:**
  - Confirmation of the existence of reasonable steps evidence referenced by SMFs during the workshops
  - SMF interviews to assess hand over arrangements in practice, if applicable

- **Walk-throughs related to:**
  - The assessment of whether a new role or colleague is in scope of the CR
  - The F&P assessment process, encompassing each component of the assessment
  - The recertification process
  - The change management process for roles or colleagues in scope of the certification
  - The controls underpinning temporary appointment to a certified role
  - The role of the compliance function, including quality assurance activities, and the provision of regulatory guidance
EY's July 2018 edition of *Internal audit in insurance – current market issues and trends* included the topic of investment strategy with a focus on nonlife or GIs, which will be the topic of this publication. The key difference in investment strategy between life and GI firms tends to be based on the time horizon and level of overall risk, which, in turn, are driven by their underlying insurance policies and approaches to managing their liabilities. Life insurers consider matching their asset strategies to their liability profiles as critical and tend to invest over a longer time horizon with a higher level of overall risk. Meanwhile, GI firms place significantly less emphasis on matching strategies, with more of their interest focused on achieving a steady investment return to contribute to overall profitability with less tolerance for loss, typically over a shorter time horizon, such as a calendar year. Subsequently, GI firms tend to take a lower level of investment risk and invest more heavily on fixed incomes or cash-style securities.

Weak investment returns in 2018 across the majority of asset classes – 90% of all asset class returns were negative for the year, which is the highest since records began – are likely to have a significant impact on GI firms' investment income and overall profitability. We expect to see a significant divergence of returns from GI firms in 2018 driven by the level of risk appetite, how diversified their portfolios were and which asset classes or parts of their portfolio they chose to place their investment bets on.
What does ‘good’ look like?

EY’s General Insurer Asset Strategy Framework below displays the key areas that should be considered within an investment framework and the typical areas of responsibility for the senior management. The second and third lines of defence, including internal audit, typically fits in the fourth section – risk and operational oversight.

Figure 1: General Insurance Asset Strategy Framework

*Investment management information reporting
**International Financial Reporting Standards
***Generally Accepted Accounting Principles
Key challenges

There are a number of key challenges faced by insurers:

- The lack of expertise in investment – Many GI firms have a lack of specific investment knowledge within their boards and investment committees as the majority of senior management and nonexecutive directors typically come from a predominantly underwriting background.
- Profitability pressures – GI firms are under pressure with regard to profitability due to weaker underwriting, and investments represent a higher proportion of net income in recent years.
- External pressures – Higher levels of M&As and pressure from the regulator are inviting more scrutiny on investment strategies.
- Risk and return – The levels of risk in GI firms’ portfolios have tended to be higher in recent years as these firms have diversified away from traditional areas of investments, such as cash and short durations, to attempt to achieve higher returns. The year 2018 has been particularly challenging as most of these nontraditional assets, such as absolute return strategies, hedge funds and equities, suffered from high levels of volatility and lacklustre returns.

What should an internal audit scope include?

The internal audit may consider the following areas within the scope of a review of an investment strategy.

Governance:

- Stakeholder structure, governance and decision-making responsibilities, including:
  - Roles and responsibilities
  - The agility with which investment decisions can be made
- Approval process for key changes (e.g., new asset classes, new managers and changes to Asset Allocation on a tactical or strategic basis)
- Guidance and challenges undertaken over the investment strategy in line with business objectives
- Process for the setting of investment beliefs
- Appropriateness of the investment policy and beliefs (in terms of definition and alignment to strategy)
- Process for the setting of risk appetite and return targets

Asset Allocation:

- Process for the generation of inputs used in strategic asset allocation
- Process for the setting of TAA limits
- Monitoring of the adherence to strategic asset allocation and TAA limits
- Review of hedging programme around currency or duration, including effectiveness

Manager oversight:

- Process for manager selection
- Monitoring process for managers
- Peer analysis undertaken for managers in relation to performance and fees
- Ensuring of operational adherence to set guidelines or objectives

Risk and operational oversight:

- Process for monitoring and managing investment risk including metrics, such as:
  - Capital, SCR and liability impact
  - Risk appetite and return targets
  - Stress and scenario testing
- Regulatory reporting
- Process for understanding, reviewing and approving complex and new asset types
Workforce-based regulations

A number of recent regulations focused on the fairness agenda, as well as trends in associated human resources (HR) policies, are driving up complex compliance obligations and reputational risks for financial services organisations.

Understanding its impact

A number of regulations focused on the workforce are designed to improve fairness at work in the UK economy and bring improvements for UK public limited companies. Organisations themselves are responding with HR policies that broadly align with this wider agenda, and seek to promote diversity, inclusivity and workplace attractiveness. These regulations and policies present organisations with a number of direct and indirect compliance obligations, which are notable for the reputational and financial risk that compliance failure can bring.

Compliance with these obligations typically sits across a number of functions, including HR, payroll and group tax; and specialist knowledge is often needed to ensure compliance and accurate reporting.

Why act?

Many workforce-based regulations are either not front and centre in the minds of HR and tax functions (e.g., National Minimum Wage (NMW) for HR and agile working for tax) leading to inattention to the details of the rules or are highly sensitive topics (remuneration policies and gender pay reporting) where internal pressures can deviate an organisation from robust implementation. The implications of failure can be costly:

1. Fines of twice the amount of underpaid wages, up to £20,000 per employee under NMW, could be levied.
2. There could be adverse media attention for improperly explained gender pay reporting or NMW breaches.
3. A number of organisations have faced costs in excess of £350,000 associated with a single employee found to be working outside their country of employment.
4. Thirty percent of contractors stopped working for their clients during the implementation of IR35 reforms in the public sector.

---

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Scope area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remuneration regulations for insurance: Effective remuneration plan design and governance are key requirements of Solvency II Directive of the EU and need to be aligned both to business performance and regulatory expectations. The PRA has provided additional supervisory statements on the remuneration requirements of Solvency II Directive applicable to Category 1 and 2 firms, although relevant for all firms in considering their alignment with the directive’s remuneration requirements. Whilst there is no requirement for the application of these to be audited, the regulatory and overall business risks for organisations, which cannot demonstrate compliance, are significant.</td>
<td>• Review of the design effectiveness of remuneration policies, processes and governance arrangements to check alignment to key regulations, including Solvency II Directive • The operating effectiveness of remuneration governance to check alignment to stated policies and effective links to company, business and personal performance</td>
</tr>
<tr>
<td>Gender pay reporting: We are in the second year of gender pay reporting obligations. These represent a profound technical and strategic challenge for organisations. The failure to properly identify the components of remuneration to be included in pay for gender pay reporting – to accurately calculate the gender pay gap given in the multiple sources from which data can be found and then to maintain consistency between years – can create a distorted perception in the marketplace of an organisation’s compliance with a regulation that receives intense media attention.</td>
<td>• Design principles, policies and procedures for calculating the organisation’s gender pay position • Process and its associated controls for the calculation of gender pay, including how accuracy and completeness are ensured</td>
</tr>
</tbody>
</table>
### Regulation

**National Minimum Wage (NMW):** The rules on NMW represent a completely separate mechanism for calculating pay from all other purposes (e.g., tax, pensions and gender pay). The notoriously complex rules have allowed Her Majesty’s Revenue and Customs (HMRC) to publish the names of many organisations for failing to pay NMW due to errors that arise from organisational ignorance or a failure to understand the zero-based tolerance that HMRC brings to the application of the rules. When an organisation fails an audit, which can be prompted by whistleblowing from a disgruntled ex-employee, the organisation is publicly named by the HMRC with the resulting media publicity for well-known brands.

Particular risk for insurance companies lies in the calculation of pay for call centre staff, professional staff on an annual salary working long hours at particular times of the year and short-term assignments to the UK from low-cost offshoring locations.

### Scope area

- Process for the calculation of pay for NMW purposes
- Controls and procedures to prevent the accidental payment of less than the NMW and associated process for rectification where controls break down
- Process for identifying individuals paid below the NMW and the resulting rectification
- Process for ensuring the understanding of HMRC’s minimum wage rules is up-to-date

### Flexible working arrangements:

Flexible working is an increasing fact of life in medium to large organisations that frequently implement formal policies encouraging the behaviour to promote their attractiveness to scarce labour pools. However, taken to its extreme, such initiatives allow employees to work from home outside the UK, triggering a number of tax and HR risks, which can lead to significant financial cost and employment risk. Financial services organisations are beginning to set up compliance programmes targeted at managing the specific risks of flexible or agile working but few have reached.

- Review of existing compliance programme for right to work, employment tax, permanent establishment and employment law; and its alignment to flexible working policy
- Review of publicity and communications associated with flexible working programme and its alignment with the compliance programme

### IR35 and contractor taxation:

From April 2020, organisations will need to take on the obligation to assess the employment status for tax purposes of many independent contractors from the contractors themselves. The underlying laws are highly contentious in the eyes of many in the UK’s contractor labour pool and the new requirement presents organisations with a competing cocktail of risks, including tax, financial and operational risk. Depending on the size of the contractor population, organisations should be ramping up programmes to manage the transition into the new regularity framework for contractor taxation with a key focus on contractor engagement if the issue is not to disrupt the delivery of key programmes.

- Review of IR35 programme for readiness ahead of April 2020 changes, including:
  - Levels of contractor engagement
  - Changes to business-as-usual onboarding processes
  - Awareness of expected cost increases
Cloud security assurance

Cloud technology is no longer an emerging issue. It has now firmly emerged and is here to stay. With many organisations adopting a ‘cloud-first’ IT strategy, and increased uptake of cloud services across financial institutions over the last 12 months, focus on the security assurance of these services continues to grow, both internally and from regulators.

Background
There are several reasons that lead organisations to invest in cloud platforms, such as challenges with end-of-life infrastructure, the desire to take advantage of opportunities to standardise and automate IT services, as well as the need to move to a pay-per-usage technology cost model.

When you consider the speed of digital transformation, and the pressure to keep pace with agile new market entrants and innovative competitors, cloud services are being used as an accelerator to develop and deploy meaningful products to an organisation’s customer base as quickly and efficiently as possible. Recent advances in business applications of advanced analytics and machine learning also mean that organisations are demanding flexible, scalable data solutions – for which cloud-hosting solutions are more financially and operationally viable to utilise than on-premise infrastructure.

Also, cloud services themselves have been maturing significantly in recent years, perhaps spurred on by publications, such as the guidance for firms outsourcing to the cloud set forth by the FCA, and other third-party IT services. Adhering to this guidance should generally indicate compliance with the FCA’s outsourcing requirements. It should cover many areas, such as legal and regulatory requirements, risk management, international standards, oversight, data security, GDPR, access to data and business premises, relationships between providers, change management, business continuity and resolution, and exit planning. These guidelines were useful not only for financially regulated firms considering moving to the cloud but also for cloud service providers looking to appeal to those potential customers by offering products that enable compliance.

As a result of this maturation, in terms of securing and controlling cloud environments, cloud services are now able to integrate with an organisation’s current security tools and processes, as well as provide opportunities to decrease manual operational activities and associated risks by operating in conjunction with automation tools. An example for the same would be provisioning, monitoring, securing privileged accounts, patching and asset management.

When you consider the above-mentioned drivers, on top of companies now being able to assess their risks, deploy and configure mitigating controls as well as monitor their cloud-hosted IT services within risk appetite, it’s no surprise that regulated industries, such as financial services have started to invest significantly in cloud-migration programmes.

Why is cloud security important?
Failures in data security and privacy continue to make media headlines around the world, and the impact of breaching regulatory obligations is widely recognised.

It should come as no surprise that the risks posed to information hosted on the cloud requires the same levels of risk management, control and oversight that is applied to on-premise IT systems. Given the active involvement and inquiries of regulators into the usage of cloud services by financial institutions, providing internal security assurance has never been more relevant.

Challenges
There are many challenges faced by organisations wishing to take advantage of cloud services, such as the following:

- Lack of skilled technical security or operational resources with cloud experience across the three lines of defence is one of the main challenges. Whilst these skills are pivotal to the secure development, integration, deployment and operation of cloud systems, including the selection and implementation of appropriate security controls, business leadership may also require ongoing assurance over the
management of information risks in the cloud. The ability
to assess and understand technical security test results,
and to translate and communicate these findings to
residual risks is key.

- Management of dependencies and priorities with
  security or operational teams whilst onboarding the new
  environment onto current tools is essential.
- Competitive and internal pressures to deliver cloud
  platforms mean that programmes often have very tight
timelines. This can lead to compromises in terms of
security requirements not being entirely fulfilled before a
production release.

**Internal audit’s approach**

Internal audit can provide assurance that cloud migration,
development and deployment are secure and sustainable
through a variety of methods either separately or in
conjunction.

Firstly, the contractual agreement with the cloud service
provider can be assessed to determine whether regulatory
requirements and notifications have been considered and
the business fully understands the service agreement with
the supplier. This includes clearly documented roles and
responsibilities, levels of support available, guidelines on the
right to audit, and an appropriate exit strategy.

Secondly, independent programme assurance can be applied
with certain aspects tailored to cloud projects. For example,
an assessment of the project’s architecture forums and
design decisions will provide insight into whether appropriate
subject-matter experts have been engaged during the process.
Additionally, it will also suggest whether appropriate security
controls have been selected and incorporated into the design
in line with broader architectural and security strategy.

Thirdly, operational readiness testing should be performed to
ensure all in-scope security controls have been implemented
effectively on the platform and applications prior to going
live in line with business policy. This can include reviewing
evidence demonstrating that:

- Access to privileged accounts has been restricted.
- Account recertification can be performed.
- Audit logs are being generated and onboarded to event
  monitoring tools.
- Workloads are encrypted and certificates are managed.
- Results of penetration testing and vulnerability scanning
  are within appetite.
- Infrastructure is being monitored and alerts generated
  when necessary.
- Firewall rules have been configured with an approval
  process in place to make any changes.
- Capacity and performance is monitored.
- Systems can be patched.
- Cloud platforms are included in asset management
  reporting.
- Disaster recovery testing has concluded, with the
  restoration of service completed in line with business
  requirements.

Consideration should be given to whether the security controls
are sufficiently automated and, therefore, scalable in the
production environment. Such testing could also include a
review of operational risks to assess whether any remaining
items have been approved by the receiving business, and that
operational teams are adequately trained and equipped to run
the service.

Lastly, a post-implementation review could be considered,
including an assessment of whether the project appropriately
handed over the operation, testing and reporting of security
controls. Control testing across the new cloud environments
should be incorporated into upcoming test schedules and
relevant risk reporting processes. The review should also make
sure that the team members have been upskilled and are able
to perform such activities.
Contacts

David Parkinson
Partner
Insurance and Wealth & Asset Management Internal Audit Lead
+44 20 7951 2318
dparkinson@uk.ey.com

David Sooby
Director
Insurance Internal Audit Lead
+44 20 7951 4940
dsooby@uk.ey.com
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.

© 2019 EYGM Limited.
All Rights Reserved.

EYG no. 003387-19Gbl
EY-000090383.indd (UK) 07/19.
Artwork by Creative Services Group London.

ED None

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com