Chartered Institute of Internal Auditors

HIAF – 31st October 2018

Chartered IIA – Hot Topics

RFC revised Corporate Governance Code
Risk in Focus 2019

Liz Sandwith CFIIA
Chief professional Practice Advisor

Chartered Institute of Internal Auditors

Corporate governance challenges / failures

Reasons for corporate failures?

- Greed
- Poor financial management
- Manipulation of financial records
- Ill advised merger and acquisition activities
- Fraudulent activity
- Incompetent management
- Over-expansion
- Excessive risk taking

✓ **Northern Rock**	✓ **BP**
✓ **HBOS**	✓ **Barclays (Libor rate)**
✓ **RBS**	✓ **Wells Fargo**
✓ **Lehman Bros**	✓ **BHS**
✓ **WorldCom**	✓ **Sports Direct**
✓ **Enron**	✓ **Carillion**
✓ **Bernard Madoff**	✓ **Oxfam**
✓ **Société Générale / Barings**	✓ **Barclays CEO re Whistleblowing**
✓ **ABN-Amro**	✓ **Patisserie Valerie**

Chartered Institute of Internal Auditors

Thoughts for today

- The FRC published the revised guidance on UK Corporate Governance Code on 16th July 2018.
- The Code applies to all listed UK companies whose accounting periods begin on or after 1 January 2019.
- Other listed or unlisted companies may wish to adopt the Code in whole or in part
- The Code puts the relationships between companies, shareholders and stakeholders at the heart of long-term sustainable growth in the UK economy
- The new Code is focussed on board effectiveness, stakeholder engagement and a company's corporate purpose and culture.

Sir Win Bischoff, Chairman, FRC, said:
"Corporate governance in the UK is globally respected and is a framework trusted by investors when deciding where to allocate capital. To make sure the UK moves with the times, the new Code considers economic and social issues and will help to guide the long-term success of UK businesses. This new Code, in its new shorter and sharper form, and with its overarching theme of trust, is paramount in promoting transparency and integrity in business for society as a whole."

Chartered Institute of Internal Auditors

Business Secretary Greg Clark said:
"Britain has a good reputation internationally for being a dependable place to do business, based on required high standards. It is right that we keep under review and update our corporate governance code to ensure the highest standards.

"That is why I supported the FRC in deciding to update their Corporate Governance Code, and I am pleased to see the revised Code.

"These changes will drive improvements in how boardrooms engage with employees, customers and suppliers as well as shareholders, delivering better business performance and public confidence in the way businesses are run. They will help the UK remain the best place in the world to work, invest and do business."

Purpose and Structure of the Code

Chartered Institute of Internal Auditors

- Over the years the Code has been revised and expanded to take account of the increasing demands on the UK's corporate governance framework.
- The principle of collective responsibility within a unitary board has been a success and – alongside the stewardship activities of investors – played a vital role in delivering high standards of governance and encouraging long-term investment.
- Nevertheless, the debate about the nature and extent of the framework has intensified as a result of financial crises and high-profile examples of inadequate governance and misconduct, which have led to poor outcomes for a wide range of stakeholders.
- At the heart of this Code is an updated set of Principles that emphasise the value of good corporate governance to long-term sustainable success. By applying the Principles, following the more detailed Provisions and using the associated guidance, companies can demonstrate throughout their reporting how the governance of the company contributes to its long-term sustainable success.
- The Code does not set out a rigid set of rules; instead it offers flexibility through the application of Principles and through 'comply or explain' provisions and supporting guidance.

Chartered Institute of Internal Auditors

New Code provisions on:

- The board's role in monitoring and assessing culture;
- Mechanisms for gathering the views of the workforce;
- Reporting on how stakeholder interests, and the other matters set out in section 172 (Companies Act 2006), have influenced the board's decision-making;
- Succession planning and board member contribution;
- Diversity and inclusion;
- The length and tenure of the chair;
- Board responsibility for identifying and assessing emerging risks (in addition to the principal risks);
- Holding periods for long-term incentive schemes; and
- Pension arrangements.

Chartered Institute of Internal Auditors

New Code principles on:

- Alignment of company purpose, strategy, values and corporate culture;
- Effective engagement with shareholders and stakeholders;
- Responsibilities of the board to ensure that workforce policies and practices are consistent with the company's values and support its long-term sustainable success;
- Consideration of the length of service of the board as a whole and the need for regular board refreshment; and
- Alignment of remuneration and workforce policies to the long-term success of the company and its values.

Chartered Institute of Internal Auditors

Audit, risk and internal control

- The detailed provisions in this section remain largely unchanged, however, the Principles have been enhanced to place greater emphasis on the board's role in:
  - establishing formal and transparent policies and procedures to ensure the independence and effectiveness of internal and external audit;
  - satisfying itself on the integrity of financial and narrative statements;
  - establishing procedures to manage risk, oversee the internal control framework, and determine the nature and extent of the principal risks the company is willing to take in order to achieve its long-term strategic objectives.
- In particular, the Code has been enhanced to address emerging risk:
  - "The board should carry out a robust assessment of the company's emerging and principal risks. The board should confirm in the annual report that it has completed this assessment, including a description of its principal risks, what procedures are in place to identify emerging risks, and an explanation of how these are being managed or mitigated."

Chartered Institute of Internal Auditors

The Code from internal audits perspective

In essence it is

- Shorter and easier to navigate
- Focused on the Principles
- Enhanced with new Principles on stakeholder engagement, alignment of strategy, culture and values, board responsibilities regarding workforce policies, refreshing the board and remuneration
- Less onerous (59 principles and provisions compared to 99 previously)

2016 Code		2018 Code	Principles
Leadership	1	Board leadership and company	A-E
Effectiveness	2	purpose	
Accountability	3	Division of responsibilities	F-I
Remuneration	4	Composition, succession and	J-L
Relations with	5	evaluation	
shareholders		Audit, risk and internal control	M-O
		Remuneration	P-R

Chartered Institute of Internal Auditors

Changes specific to internal audit

Principle M requires the board to *establish formal and transparent policies and procedures to ensure the independence and effectiveness of internal and external audit functions and satisfy itself on the integrity of financial and narrative statements.*

- Heads of internal audit (HIAs) without a direct reporting line to the audit committee should use this principle as a discussion lever to effect change with their audit committee chair. For additional information on what constitutes 'independence' refer to the International Professional Practices Framework (IPPF) Standard 1110.
- The principle also introduces formality to ensuring the effectiveness of internal audit that was missing from the previous Code. Again this is an area where the board may need support as to how they can achieve this with minimum effort given the limitations on their time.

Chartered Institute of Internal Auditors

- Audit leaders may wish to think about preparing a policy and approach for their audit committee building on existing practices and incorporating the IPPF which sets out ongoing review Standard 1300 (quality assurance improvement programme), internal assessment Standard 1311 and external assessment Standard 1312.
- Establishing KPIs to measure performance may also be useful.
- HIAs must give consideration to the assurance provided over the narrative statements in the annual/interim report, reports to regulators, price-sensitive public records and other information required by statutory instruments.

Chartered Institute of Internal Auditors

Supporting Principle M is **Provision 25** requiring the audit committee to *monitor and review the effectiveness of the company's internal audit function or, where there is not one, considering annually whether there is a need for one and making a recommendation to the board.*

- This is not new and you may be disappointed that the provision does not make internal audit compulsory.
- The Institute maintains open dialogue on this point.
- It therefore remains incumbent on the internal audit profession to educate and support audit committee chairs on the value that internal audit delivers.
- HIAs should not take for granted that whilst their organisation currently has an internal audit function; it can be outsourced or removed with reasonable explanation due to budget constraints, downsizing etc.
- Whether supplemented by formal processes or not, the audit committee forms its opinion of internal audit effectiveness through ongoing dialogue with the head of internal audit and the board/senior management together with the content and presentation of regular reports.
- HIAs may find this an opportune time to evaluate their relationships and review their audit committee reporting; its frequency, content, format and readability.
- Does it provide insight and information or data?
- Does it generate meaningful discussion or is it largely nodded through the agenda?
- Does it inspire confidence in the function?

Chartered Institute of Internal Auditors

Corporate Culture

- The new Code states that *a company's culture should promote integrity and openness, value diversity and be responsive to the views of shareholders and wider stakeholders;* in the wake of scandals this clearly aims to rebuild corporate trust.
- **Principle B – Provision 2** requires the board to assess and monitor culture, and report on it in the annual report.
- Where will the audit committee seek such assurance?
- How will internal audit know that management need to take action?
- Audit committees should be discussing this with internal audit. They should be challenging HIAs that have made no provision for assurance on culture. Whether specific audits, integrated into all audits or following up on specific actions, it must be addressed.
- Audit leaders have long recognised the significance of culture to organisational success, as a minimum HIAs should consider their assurance provision over the sources that boards are being encouraged to look at by the FRC.

Sources of culture insights

- Turnover and absenteeism rates
- Training data
- Recruitment, reward and promotion decisions
- Use of non-disclosure agreements
- Whistleblowing, grievance and 'speak-up' data
- Employee surveys
- Board interaction with senior management and workforce
- Health and safety data, including near misses
- Promptness of payments to suppliers
- Attitudes to regulators, internal audit and employees
- Exit interviews

Extract from 2018 FRC Guidance on Board Effectiveness

Chartered Institute of Internal Auditors

Internal Audit opportunities

- The 2018 Code provides numerous opportunities for audit leaders to engage with the board and audit committee and demonstrate the value that internal audit can bring to an organisation.
- Board evaluation is not a new concept; although it is rarely undertaken by internal audit.
- Could internal audit have a role in assuring the board over their processes such as appointments and succession planning for example?
- Does this have to be outsourced to external consultants?
- Would more frequent assurance be beneficial to boards going through change?
- Assurance from culture to pay ratios,
- Board appointments to emerging risks, internal audit has a role to play.

Chartered Institute of Internal Auditors

5 Key questions for internal auditors

Stakeholder understanding of internal audit's role in good governance is essential to making best use of a vital governance tool. Are you able to answer these questions?

1.How deeply is internal audit involved in the organisation's discussions on risk?

2.Is internal audit properly positioned and resourced to provide high-quality, professional assurance and advisory services?

3.Is the head of internal audit free to develop strong relationships with the board and/or audit committee chair?

4.Does the board/audit committee recognize and support the best conditions under which internal audit can thrive?

5.How can management and the board support efforts to make the internal audit activity agile and innovative?

Source: IIA Global

Chartered Institute of Internal Auditors

Internal Audit Key Take-aways

1. Internal audit's role in governance is vital. Internal audit provides objective assurance and insight on the effectiveness and efficiency of risk management, internal control, and governance processes.
2. Internal audit insights on governance, risk, and control provoke positive change and innovation within the organisation.
3. Strong management and board support of internal audit is nurtured by relationships built on mutual trust and frequent and meaningful interactions with the HIA.
4. A vibrant and agile internal audit function can be an indispensable resource supporting sound corporate governance.

Source: IIA Global

Chartered Institute of Internal Auditors

What is next on the agenda?

✓ The Kingman review of the FRC which is a root and branch review, is due for completion by the end of 2018, and will assess the FRC's governance, impact and powers, to help ensure it is fit for the future. The review aims to make the FRC the best in class for corporate governance and transparency, while helping it fulfil its role of safeguarding the UK's leading business environment.

✓ James Wates CBE will lead the development of corporate governance principles for large private companies. The appointment, announced by Business Secretary Greg Clark, is part of the Government's package of corporate governance reforms, and will involve work with the Financial Reporting Council, the Institute of Directors, the Trades Union Congress and others to help improve the way private companies are run in the UK.

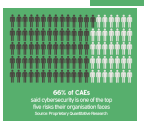
Chartered Institute of Internal Auditors

- Risk In Focus 2019
  - Cybersecurity: IT Governance and Third parties
  - Data Protection & Strategies in a Post-GDPR World
  - Digitalisation, Automation & AI: Technology Adoption Risks
  - Sustainability: The Environment and Social Ethics
  - Anti-Bribery & Anti-Corruption Compliance
  - Communications Risk: Protecting Brand & Reputation
  - Workplace Culture: Discrimination & Staff Inequality
  - A New Era of Trade: Protectionism & Sanctions
  - Risk Governance & Controls: Adapting to Change
  - Auditing the Right Risks: Taking a Genuinely Risk-based Approach

Cybersecurity: IT Governance & Third Parties

Chartered Institute of Internal Auditors

- Cybersecurity has been a high-priority risk for a number of years and this shows no signs of abating.
- Companies are pushing to move away from legacy systems and, as approaches to managing cyber risk mature, attention is turning to third-party defensibility
- Cybersecurity risk is here to stay and the third line of defence will be expected to provide assurance on the internal management of this risk for the foreseeable future, if not indefinitely



Key Questions:

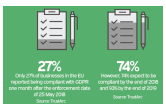
Chartered Institute of Internal Auditors

- Has the organisation moved or is it moving away from legacy systems to a more homogeneous, harmonious system that is easier to defend?
- Are security considerations central to the IT plan and network development?
- Is there strong governance in IT and oversight of procurement and development of networks and infrastructure?
- In addition to having robust defences to keep attackers out, does the organisation deploy effective monitoring capabilities to detect when a breach has occurred?
- Is internal cyber risk management sufficiently mature to direct attention towards connected parties?
- What cloud services does the company use and how is the organisation sure these providers maintain high security standards and robust controls?
- Are the same password management standards applied internally also applied to cloud services?
- How strong are the procurement function's cybersecurity due diligence processes when bringing on board suppliers and connecting with business partners

Data Protection & Strategies in a Post-GDPR World

Chartered Institute of Internal Auditors

- The deadline for the EU's General Data Protection Regulation has now passed and internal audit functions have either performed readiness audits or will imminently look at this area for the first time.
- But there is more to consider than simply ticking the GDPR compliance box.
- For many companies, particularly those for which personal data is central to revenue generation, this will require periodic reviews, especially as new data points are harvested and by new means, e.g. collecting personalised customer behaviour data through geolocated advertising that interacts with people's smartphones.



Chartered Institute of Internal Auditors

Key Questions:

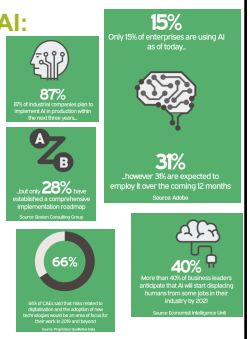
- Is the organisation compliant with GDPR and, if necessary, China's Personal Information Security Specification?
- Are US companies that share the organisation's personal data certified under the EU-US Privacy Shield scheme?
- How is personal and operationally/strategically sensitive data shared with third parties and how do you know these parties are keeping it secure?
- Is the compliance function in close communication with the data management function so that the former is aware of how any company changes may impact upon GDPR compliance?
- Is there a data strategy for how the organisation uses data, personal or otherwise, to its advantage? Is this aligned with the corporate strategy?
- How does the strategy envisage data being used in the future? Is this clear and well articulated?
- Is the internal audit function prepared to advise the Chief Data Officer and/or data management function with any changes to the organisation's use of data by providing a risk control perspective?

Similar Risk as 2018

Chartered Institute of Internal Auditors

Digitalisation, Automation & AI: Technology Adoption Risks

- The cost and efficiency benefits of automation and other digital processes can be transformative, if harnessed to their full potential.
- But organisations must also consider the risks associated with such transformation.
- Senior management and the board should be aware of the risks associated with adopting new technologies.
- There may be value in the organisation assessing how direct competitors are adopting new technologies, how successful this has been for them and why, and whether the market has reacted positively to such development.



Chartered Institute of Internal Auditors

Key Questions:

- What different technologies are being adopted? Is there a clear, documented rationale for doing so that is consistent with the organisation's broader operational and strategic objectives?
- Who is accountable for these projects and are they taking into account the potential risks that come with digitalisation?
- To what extent will new technologies require updates and modifications to the control environment? Is the first line making these control changes?
- Is there enough buy-in and sponsorship from middle management to give technology adoption the required momentum to be successful?
- Is there resistance to digitalisation in the workforce and is it negatively impacting culture? If so, what steps can be taken to measure and remediate this?
- Are automated processes being risk assessed for data quality, the accuracy of algorithms and outputs and is internal audit equipped to confirm that technologies are working as intended? If not, who is providing this independent assurance?

New Risk for 2019

Chartered Institute of Internal Auditors

Sustainability: The Environment and Social Ethics

- Companies are increasingly expected to behave in an environmentally and socially responsible manner, both by regulators and the public.
- This is creating sustainability reporting challenges and is influencing the strategic decisions companies must take to achieve future growth.
- Organisations must now report on what they are doing to identify and mitigate sustainability risks and should look to the Global Reporting Initiative's Sustainability Reporting Standards (GRI Standards) for guidelines on how to achieve this

Chartered Institute of Internal Auditors

Key Questions:

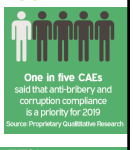
- Is the organisation publishing non-financial reports as required by the EU?
- Is there scope for internal audit to assess the maturity of sustainability reporting and review the extent to which the company's environmental and social ethics statements reflect reality?
- Does the organisation benchmark sustainability performance against sector-specific KPIs? Is there a gap between both the organisation's sustainability reporting and performance compared with that of its industry peers?
- Is the organisation complying with all relevant environmental laws in all territories?
- To what extent is tightening environmental regulation likely to impact the company's strategy, e.g. targets to reduce carbon emissions? Is senior management aware of this likely impact?
- Does senior management understand the importance of continuously improving operations in order to minimise environmental and social harm?
- Is there value in internal audit assessing progress and providing evidence of relevant sustainability improvements?

New Risk for 2019

Chartered Institute of Internal Auditors

Anti-Bribery & Anti-Corruption Compliance

- Anti-bribery and corruption (ABC) risk is longstanding; however, national legislative reforms, coordinated global enforcement by regulators and record-breaking fines are raising the stakes and pushing this issue to the top of the corporate agenda.
- The introduction of ISO 37001, the first international anti-bribery management system standard, in 2016, set out a number of measures that companies can take to prevent and detect bribery.
- Internal audit should evaluate the design of the organisation's anti-bribery and corruption programme for completeness



Chartered Institute of Internal Auditors

Key Questions:

- Does the organisation have an all-inclusive and effective antibribery and corruption programme?
- Is there a zero-tolerance statement from management?
- Are there staff awareness and training programmes and an established whistleblowing procedure?
- Does an anti-bribery culture permeate the organisation?
- Has a risk assessment been conducted on the organisation's exposure to bribery and corruption?
- Is second line activity sufficiently risk-based and directed at territories and business units most exposed to bribery risk?
- Has senior management considered whether to become ISO 37001 certified? If not, against which guidance/framework does the organisation benchmark itself?
- Is there a segregation of duties regarding facilitation payments to agents and advisers, and are due diligence policies for bringing on board third parties followed in practice?

New Risk for 2019

Chartered Institute of Internal Auditors

Communications Risk: Protecting Brand & Reputation

- The risks associated with brand and reputational harm have become more prominent as high-profile mistakes continue to be made in the public forum. Companies must think carefully about how they present themselves.
- Senior management and the board should be aware of the importance of brand value and the principle that a reputation takes years to build and only minutes to tarnish.
- Documented communications guidelines and policies for what can be said and what should be avoided help to mitigate risk.

Key Questions:

- Is the board and management aware of the potential reputational harm caused by poor communications?
- Who is responsible for the organisation's various communications channels and do they acknowledge their accountability?
- Are marketing staff aware of brand guidelines, the organisation's "voice" and what can and can't be said, e.g. policies around engaging in political debates?
- Are policies around what can and can't be said and the segregation of roles and responsibilities documented?
- Are access rights appropriately managed, e.g. changing social media account and corporate blog passwords when people leave the company?
- Is there a crisis response plan in place that involves both the CEO and the communications function?
- Does the organisation engage in communications scenario practices and are lessons learned from competitors' mistakes?
- Does the organisation have media training in place for those employees required to deal with the media e.g. CEO, Chairman?

According to the Reputation Institute, there are seven dimensions of reputation that impact the way people perceive companies. These are:

Leadership
How is your company leading the way? Companies with CEOs and senior executives who take a stand on critical, often controversial, issues tend to outperform those companies that remain silent.

Performance
Numbers matter. Performance and profitability are key indicators of reputation success.

Products
Consistent delivery of quality products and services determine a company's value.

Innovation
Is your company static or dynamic? Innovative companies that creatively push the status quo are more highly regarded.

Workplace
Corporate culture directly impacts recruitment, retainment, and the quality, ability and willingness of companies' greatest asset — human resources — to deliver on strategy.

Governance
Only with stakeholder support from those providing your company a licence to operate and benefit of the doubt will result in continued growth.

Citizenship
How does your company add value above and beyond delivering products and services? Corporate social responsibility, charitable giving, volunteer efforts, and philanthropic campaigns help to make the world a little better.

Similar Risk as 2018

Chartered Institute of Internal Auditors

Workplace Culture: Discrimination & Staff Inequality

- Widespread allegations of the mistreatment of female actors in Hollywood emerged in 2017, giving rise to the #MeToo movement.
- While harassment in the workplace and society at large is not new, the pressure for this to change has never been greater, owing to the use of social media to spread global awareness of this issue.
- Regulatory requirements are increasing with regards to the fair treatment of staff. In Europe this has centred around disclosures in company reports, so at a fundamental level internal audit can assist in ensuring that organisations are compliant, i.e. that, at the very least, the gender pay gap has been reported and published ahead of the deadline

25% of CAEs say that culture is one of the top five risks their organisation faces..

10% say they anticipate that internal audit will focus more attention on discrimination and the fair treatment of staff going forward

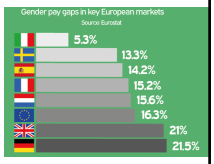
Source: Proprietary Quantitative Research / Proprietary Qualitative Research

28%
The gender pay gap in the financial services sector across the EU is 28%, higher than in any other industry
Source: Eurostat

Key Questions:

Chartered Institute of Internal Auditors

- Are senior management and the board paying sufficient attention to the shift in society regarding the fair treatment of women and other marginalised demographics?
- Have management set an appropriate 'tone at the top' with respect to harassment?
- Does the organisation have a clear and adequate antiharassment policy in place?
- Is the organisation obliged to report on its gender pay gap (250 employees)? If so, is it compliant? And is the data accurate?
- Does HR communicate this policy, raise awareness among staff and effectively record and follow up on accusations of mistreatment?
- Does internal audit undertake audits that take into account culture? If so, is there scope to include surveys and other assessments that can shed light on how staff are treated within the organisation?



New Risk for 2019

Chartered Institute of Internal Auditors

A New Era of Trade: Protectionism & Sanctions

- The recent rise of protectionist trade policies poses a significant risk to businesses.
- The US has engaged in a tit-for-tat with China over the competitiveness of imports which has spilled over to Europe and has the potential to depress sales into the US, the world's largest economy.
- Added to this burden is an increase in trade sanctions that carry heavy penalties.
- It is debatable whether trade protectionism and export sanctions, and geopolitics more generally, are auditable risks
- However, the ability of the organisation to respond to the policy changes and put into effect contingency and mitigation strategies is something internal audit can provide assurance on

7,000 protectionist trade measures worth $400bn were introduced in the eight years following the financial crisis. This does not account for the recent raft of measures imposed by Trump, which includes 25% tariffs on $50bn worth of Chinese goods.

Source: Gowling WLG

Key Questions:

- To what extent is the organisation likely to be affected by trade tariffs and in what way, e.g. direct impact on revenues and/or input costs, disruption to the supply chain? Is senior management aware of this?
- Is the organisation flexible enough to adapt to these changes, e.g. by reducing prices to remain competitive, or are revenues sufficiently hedged across markets such that the impact of US tariffs will be minimal?
- Does the supply chain need to be restructured or can the organisation withstand potentially higher costs and keep things as they are?
- Is the organisation responding to trade policy changes by conducting regular risk assessments?
- Are the compliance and procurement functions updating the trade sanctions register and ensuring that it is being complied with across the organisation?

Similar Risk as 2018

Risk Governance & Controls: Adapting to Change

- The pace of change to businesses' operations and the risks they are exposed to has never been faster.
- As organisations adapt to achieve growth, risk governance standards and control environments that were designed to mitigate yesterday's risks can quickly become outdated.

"We are striving for a real **simplification** of the control environment. Currently the control system is **too complicated** and with too much emphasis on legality and conformity. With our new integrated IT system and new organisational procedures, it's the right time for all stakeholders to put everything on the table to try and find smarter, more **fluent controls** for the operational engine."

Chief Audit Executive, French public sector

Key Questions:

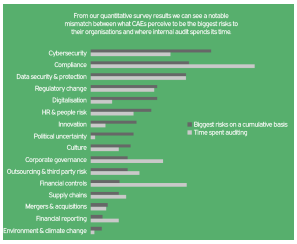
- What is the overall quality of risk governance and management, e.g. is the second line generally effective, what does it do on a day-to-day basis and is it responsive to change?
- Has the organisation undergone, or does it intend to undergo, significant change in the last/next three years? What is the change (joint venture, digitalisation, app development etc) and does the internal control framework need to be adapted accordingly?
- Is control design and implementation responsive to changes and growth in the organisation?
- How is the adoption of technology impacting upon the control environment?
- Are ineffective and redundant controls that provide little value in mitigating risk dropped or replaced?
- Is internal audit able to stay on top of organisational change and the resulting impact on the control environment?
- Does the organisation engage in agile development methods and are they delivering results whilst mitigating future risks? Is this agile activity effectively coordinated or is it siloed and scattered?
- Can internal audit add value by advising on risk considerations early in development processes?

New Risk for 2019

Chartered Institute of Internal Auditors

Auditing the Right Risks: Taking a Genuinely Risk-based Approach

- There is a notable inconsistency between organisations' priority risk areas and where internal audit focuses its time.
- CAEs should therefore re-evaluate with their audit committees and stakeholders whether internal audit is being used effectively to deliver sound risk-based assurance.



Key Questions:

Chartered Institute of Internal Auditors

- As the CAE, are you confident that internal audit's time is being effectively matched to the organisation's biggest risks?
- If there is an observable discrepancy, what is the explanation for this? For example, is assurance coverage provided by another function?
- Is there a difference between boards'/audit committees' and CAEs' perception of the greatest risks to the organisation? If so, why and is this addressed and challenged on a regular basis?
- As the CAE, do you have a risk based strategic internal audit plan that is reviewed at least annually and shared and discussed with the audit committee?
- Is there potential to increase data analytics capabilities to achieve continuous auditing for more mature risk areas, e.g. financial controls?
- Are internal audit activities coordinated with other internal and external assurance providers to ensure proper and appropriate coverage?
- Is there an assurance map that clearly documents accountability for assurance across the organisation's key risks?
- Is the internal audit function undertaking second line duties and responsibilities that undermine its objectivity and pull its focus away from key risks that lack assurance coverage?

Chartered Institute of Internal Auditors

Chartered Institute of Internal Auditors

We'd love to hear from you…

Liz.sandwith@iia.org.uk

Chartered Institute of Internal Auditors, UK and Ireland, official group

@CharteredIIA