



## Regulatory complexity and uncertainty



Uncertainty is the only certainty there is, and knowing how to live with insecurity is the only security. Prophetic words from mathematician John Allen Paulos that resonate as we emerge from a global pandemic and in the changing and uncertain world of corporate regulation and legislation.

Uncertainty of itself is not the issue. The issue arises when decisions have to be made, choosing a course of action based on incomplete knowledge. For auditors who gather evidence to form an objective opinion, uncertainty is the antithesis.

This guidance will briefly explore the complex regulatory landscape that chief audit executives (CAEs) have to navigate and consider how the complexity and uncertainty of such change can be managed. It is sector-generic and by looking across rather than into the detail, there may even be a nugget of new insight for seasoned CAEs from highly regulated industries.

---

## Regulatory landscape

Uncertainty is one quarter of the **VUCA** acronym: Volatility, Uncertainty, Complexity and Ambiguity. The buzz phrase within risk management circles and relevant for compliance today and the challenges that face CAEs.



Source: *Harvard Business Review* January–February 2014 Issue

Whether it is new accounting standards, changes to LIBOR, governance reform, reporting modern slavery or Brexit, CAEs cannot avoid regulatory and legislative change. The growing awareness of the need for good governance of organisations, society and the planet mean that the trend is unlikely to abate for increased compliance with mechanisms that direct and control the actions of others.

Ten years ago, many CAEs would have been content to carry out a compliance audit having given the organisation sufficient time to embed any new requirements. Today, CAEs are proactive and using insightful leadership skills to drive the compliance assurance agenda regardless of VUCA:

- Divide up scenarios/challenges into manageable tasks
- Build trust in the expertise of others, particularly the 2nd line defence
- Avoid reliance on existing controls and processes – look for new solutions
- Learn the value of stress management techniques - VUCA is uncomfortable

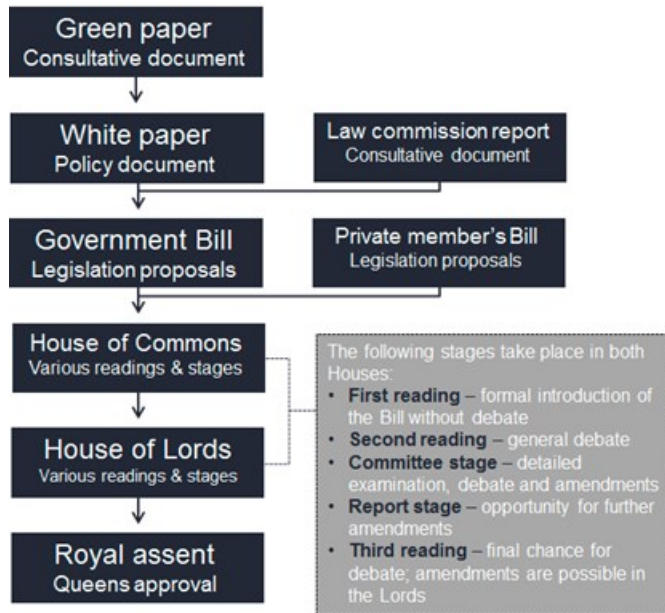
## Legislative process

The UK has a clear process for introducing new legislation which CAEs should be aware of.

At all stages, documents are publicly available and the lengthy timelines outlined. 100s of 'bills' are proposed each year, but very few make it to legislation. Once royal assent is given it becomes an Act and law.

Green papers are consultative and organisations are well advised to be members of relevant bodies, lobby groups, etc, to be able to contribute and shape future government policy.

Regulators all have their own processes although consultation is common practice.



## Assurance and regulatory change

In an age of prolific communication media, expert and disruptive commentary vie for attention as seen with the now common phrase **fake news**. Stakeholders within an organisation, particularly at a senior level, rely on objective, independent CAEs to assure them of fact vs conjecture at every stage, supporting governance and providing insight at the top table.

In a highly regulated industry, CAEs are integral to the compliance programme and the change management process, in non-regulated sectors however, CAEs have a choice in how to approach change in the compliance arena:

- Offer consultancy services to help design new controls, facilitate workshops, advise on risk management options, care must be taken not to create a conflict of interest for later compliance assurance
- Conduct a readiness review to provide assurance that compliance will be achieved, allowing sufficient time for remedial action
- Schedule a compliance review as part of routine audit planning, or advising of assurance gap depending on other priorities; and
- A combination of all or some of the approaches

The decision should factor in the complexity of the change, compliance history of the relevant function, tenure of the head of the function, risk appetite, tone at the top, velocity of the change and proportionality of the risk versus other assurance requirements.

The first line, management, is accountable for adapting or introducing controls to ensure all applicable requirements are complied with. It is not the responsibility of CAEs to be leaders in this regard if the **three lines** are working effectively.

A strong, positive culture makes it easier to adapt to change. Having open communications, seeking

solutions, clear accountabilities, a defined risk appetite, balanced strategic objectives and critically effective governance mechanisms. CAEs in organisations that face frequent compliance change either from the regulatory environment or due to expansion into new territories and/or product types may find it beneficial to look at the traits associated with a **learning culture** as it supports adaptability.

Learning organisations are most likely to anticipate change, be aware of or take an active role in consultations and integrate change through established risk management practices and governance that drives performance forward.

Alternatively, those with a less mature learning approach may respond individually to each change, reacting to what is required and managing through the disruption rather than use it as an opportunity to also improve performance and build capability. CAEs have a professional role in promoting positive cultural attributes such as continual learning.

Organisations have a choice in how to approach regulatory change depending on the degree to which the industry is regulated or has requirements that need to be maintained. The well-established **infrastructures in financial services** may provide useful learnings for others; a generalised suite of options is provided below.

	Definition	Benefits	Challenges
<b>Specialist</b>	Subject matter experts identify & manage regulatory change ad-hoc	Speed of awareness	Silo approach
		Competence	Not all stakeholders involved
		Accountability	May negatively impact others
			Reliance on limited resource
<b>Central</b>	Single function accountable for identifying & project managing change	High level of expertise	Devolved accountability
		Retained learnings	Fully engaging SME's
		High profile/commitment	Inappropriate prioritisation
<b>Embedded</b>	Regulatory change input into regular risk management/improvement cycle	Change is continual	Benchmarking performance
		Minimised disruption	Meeting deadline

The dynamics of the compliance framework is a challenge for CAEs. Is the organisation always playing catch up? How much reliance can be placed on the first and second line? Does something important get dropped to prioritise legal and regulatory demands? Complexity increases still further with international operations and the divergent requirements of different countries.

## Decision making under uncertainty

IPPF standard 2120 requires internal audit to evaluate the organisations risks regarding compliance to laws and regulations. CAEs must, therefore, be able to offer advisory services to their organisations in advance of compliance checks.

Uncertainty is a mismatch between the available knowledge and that required to make an informed decision. Obtaining the missing knowledge achieves surety. The following steps may help a CAE to begin

to do this while waiting for the legislative advice to be written; after all, the clock will be ticking. Leaders must be decisive, including CAEs. As Theodore Roosevelt said: "in any moment of decision the best thing you can do is the right thing, the next best thing is the wrong thing, and the worst thing you can do is nothing."



## Staying ahead of the curve

It is difficult for a CAE to have a constructive assurance discussion when behind the curve. Here are some simple tips for ensuring that you stay at least in sight of the curve, if not ahead of it.

- Identify your main regulators/ trade bodies and subscribe to their website, publications, etc
- Create an inventory of regulatory obligations and their risk owner
- Be clear on who is accountable for regulatory intelligence. Perhaps delegate stakeholder management to members of the team to stay up to date and share with the team
- Create an annual timeline showing effective dates for regulatory and legislative changes, with assigned owners and an impact assessment in terms of severity
- Read regulatory updates and guidance on Big4 websites and talk to an EA partner
- Connect regularly with colleagues who have responsibility for lobbying, etc
- Encourage the first line to automate controls wherever possible
- Maintain a regulatory compliance dialogue with the board/audit committee
- Check what is scheduled by parliament in the [Queen's speech](#)
- Stay abreast of current affairs and potential areas of governance concern
- Monitor the robustness of the second line/subject matter expertise – are they competent and sufficiently funded, with an appropriate turnover rate?
- Be aware of enforcement actions/breaches. Some are published (e.g. FCA for financial services, SFO for bribery and corruption, ICO for data breaches) others will be via networking
- Hold breakfast meetings to bring subject matter experts together to network

Many of these activities are easily delegated within the team, encouraging research, analysis and networking skills.

## Closing thoughts

Regulatory and legislative change cannot be avoided. Rather than thinking of requirements as something to be enforced, change the language and talk about them as enablers for success. Non-compliance is not a viable option; even where there is a tolerable financial cost, the reputational costs can be ruinous. The focus for CAEs must be on positive, adaptive leadership to maintain a healthy balance of assurance and advisory services to the organisation.

*"People lose their way, when they lose their why"*

- Michael Hyatt, Author