Key learnings from regulators for internal audit leaders

The UK's regulatory regime is considered to be one of the strongest in the world with numerous regulators across non-ministerial departments, agencies and other public bodies. In this article, we look at what internal audit leaders can learn from regulators and what insights we can take from the regulatory horizon to inform the internal audit profession.

Shared values

The third line in the Three Lines Model is about independence.

Internal audit operates at the third line complemented by regulators and other external assurance providers. Across all sectors, regulators impact the governance, risk management and internal control world of organisations and therefore internal auditors.

Click here for a useful list of regulators, available in our Templates & Tools section for reference.

Internal audit and regulators protect people and organisations by enforcing standards, advising on best practice and constructively addressing problems. Additionally, some regulators have economic responsibilities by promoting competitive forces in industries where monopolies can easily form such as CMA, Ofgem, Ofcom and Ofwat. Here in the UK, the internal audit profession is chartered, a status reserved for bodies that work in the public interest according to the Privy Council.

Regulators are bound by the Regulators Code which requires a risk-based approach, impartiality, gathering

of evidence and clarity of communication among other attributes similar to the elements contained within the internal audit standards, and Code of Ethics.

Although regulators obviously have formal power, internal auditors share the same ambition to improve through influence and developing a partnership approach with governance leaders. Organisations can and often do use the assurance provided by internal auditors as an internal early warning mechanism to validate first and second line compliance activities, and potential regulatory breaches.

Right-touch regulation

CAEs work hard to build effective relationships to ensure that internal audit delivers against its charter in a practical and pragmatic way. Firmly consigning the policeman image of yesteryear to history. A challenge also faced by regulators.

The concept of right-touch regulation was created in 2005 by the Professional Standards Authority for Health and Social Care. It is now used internationally and across a variety of regulatory sectors.

Right-touch is all about balance.

Adding more weight tips the scales, making additional regulation a burden and ineffectual. The same is true of internal audit recommendations/agreed actions – being efficient and effective. Too little is ineffective; too much is a waste of effort and is inefficient.

The regulators 'right touch' approach is based on six principles and eight steps. Each of the principles and steps has a reach across to the internal audit core principles.

See if it resonates with you.

Right touch – The six principles		
Principle	**Regulators**	**Internal audit – read across to Core Principles and attributes**
Proportionate	Intervene when necessary - remedies should be appropriate to the risk posed, and costs identified and minimised	*Principle 4: Aligns with the strategies, objectives, and risks of the organisation* *Principle 8: Provides risk-based assurance* Recognition of risk appetite Risk assessment

Consistent	Rules and standards must be joined up and implemented fairly	*Principle 2: Demonstrates competence and due professional care* *Principle 6: Demonstrates quality and continuous improvement* Standards and Practices Quality assurance and improvement programme External quality assessments Collaborative three lines approach
Targeted	Regulation should be focused on the problem, and minimise side effects	*Principle 10: Promotes organisational improvement* Root cause analysis Data analytics
Transparent	Be open, and keep regulations simple and user friendly	*Principle 1: Demonstrates integrity* *Principle 7: Communicates effectively* Code of ethics Trusted advisor
Accountable	Be able to justify decisions, and be subject to public scrutiny	*Principle 3: Is objective and free from undue influence (independent)* *Principle 5: Is appropriately positioned and adequately resourced* Evidence-based decision making Objective Independent reporting line into the governing body (audit committee)
Agile	Forward looking to anticipate change rather than looking back to prevent the last crisis from happening again	*Principle 9: Is insightful, proactive and future focused* Foresight and insight Horizon scanning Lean and agile methodologies

- Does your audit strategy reflect the Core Principles elements?
- What can you learn from the right-touch principles?
- Are all of your interventions necessary and timely?

Right touch - eight steps to effective regulatory decision-making	
Regulators 'right touch' steps	**Internal audit – read across to ways of working**
(1) Identify the problem before the solution	Take time to describe and understand a problem, process or control weakness, or failure before deciding what solutions might work. This is particularly important if you've had experience of the problem elsewhere or it has occurred before – there may be different factors this time. Root cause analysis is an objective way of looking at the problem.
(2) Quantify and qualify the risks	Understanding the risk management framework and the organisations risk appetite, using risk registers and where appropriate making an independent evaluation. Look at how a risk is being managed or if new/changed, what current options can be applied before considering novel solutions.
(3) Get as close to the problem as possible	Both professions recognise that problems are best solved where they occur. Policy, rules and regulations are distant controls. This is the value of root cause analysis and data analytics to get to the heart of the issue.
(4) Focus on the outcome	Internal audit also focuses on outcomes by using root cause analysis, ensuring agreed actions address the issue not the symptom for long-term positive outcomes. For instance, an action to include non-attendance at committee meetings is about process rather than understanding - seek to understand why members are not attending and address those issues.
(5) Use regulation only when necessary	Embedding audit actions in existing ways of working, adapting and collaborating can lead to faster and more sustainable solutions than introducing new policies and procedures. The powerful influence of internal audit, such as referral to the audit committee, should be reserved and used as a last resort.
(6) Keep it simple	For regulation to work it must be clear to all those impacted. The same is true of internal audit. The Chartered IIA leads the profession but all internal auditors and especially CAEs are responsible for advocacy. A well communicated charter, intranet page and communications are essential.
(7) Check for unintended consequences	Organisational systems are often interconnected and complex. Addressing one risk can exacerbate existing risks or create new ones. Before committing to a solution, it is important to take a moment to assess its impact.

(8) Review and respond to change	Uncertainty, volatility and change are constants. CAEs are moving away from fixed annual plans to more flexible rolling plans based on regular reviews of assurance needs. Responding to changing expectations may also require adapting ways of working to maintain relevance. Internal audit's consultancy/advisory work enables a rapid response to change along with real-time assurance.

- How do these eight steps compare to your audit methodology?
- Is there something you could improve? Add it to your QAIP today.

Learning from regulators

We know that our own experiences and events shape our personal learning. We can also learn from our peers and others. Here are three regulatory tales for you to think about.

Learning 1: People in glass houses

In December 2018, the Financial Conduct Authority (FCA) having reviewed complaints about London Capital and Finance (LFC) directed them to withdraw misleading advertising of a high-risk investment product. LFC did not take action and subsequently entered administration leaving thousands of investors out of pocket to the tune of c£237m. A Treasury Committee inquiry found that despite having the power to intervene the FCA's own polices and culture had led them to be risk averse when they needed to be more interventionist.

Ministers commented that "*there are doubts as to whether the FCA board has met the standards which it seeks to impose on others. It is not readily justifiable for the FCA … not to apply similar principles internally when there are failings of practice and culture in the organisation*."

No organisation, or function sets out to have a poor culture, it creeps up on them and like bindweed infiltrates even the most positive ways of working. Internal audit, as with regulators is dependent on the actions of individuals, the tone from the top and the day-to-day execution.

- What is the culture of your internal audit function?
- Are agreed audit actions completed in a timely fashion?
- How effective is your follow up process?

Learning 2: Too much of a good thing

Regulators are not omnipotent. Since the turn of this century serious failings in regulated sectors have touched lives and hit headlines – Stafford Hospital, Grenfell Tower, Carillion and the financial crisis. The relationship between compliance, complacency and courage is important to avoid providing false assurance and giving false comfort to governance leaders.

Compliance alone is insufficient if the rules of the game are inappropriate or outdated. Likewise, just because something has always been known to be wrong and is tolerated doesn't make it right.

Reflect for a moment on the collapse of construction giant Carillion. The public inquiry found that Deloitte, outsourced internal audit provider *'failed in its risk management and financial controls role, [they] were either unable to identify effectively to the board the risks associated with their business practices, unwilling to do so, or too readily ignored them.'* Evidence cited included the audit committee not being advised of material concerns that management had not acted upon, rarely identifying issues as a high priority nor reporting controls as inadequate.

- It is surprisingly easy to deliver false assurance. Could you have done this?
- What are the steps in your methodology to mitigate it happening?

Learning 3: Old dogs and new tricks

"Humbleness and openness" words familiar to audit leaders were a key feature of an interview for the OECD Nuclear Energy Agency in March 2021. The words of **Olivier Gupta, Director-General of France's nuclear safety regulator, will resonate with CAEs across all sectors.**

"We are working on issues for which we should never rely on certainties and this has to do with a questioning attitude, which is one of the bases of safety culture," Gupta said. "We have to expect to be challenged, and again it has to do with openness, and that's also a reason why I very much like having international exchanges. I think they too are a cornerstone of nuclear safety. Even if you belong to an advanced nuclear country, then you are prepared to change your practices, your regulations, if you identify a better practice, a better way to regulate, in another country."

- Substitute an *advanced nuclear country* for a robust governance regime – is that you?
- Are you open to learning?
- Do you listen to peers at events or actively engage in discussion to explore new possibilities?

Regulatory change

The regulators lessons are informative but they are also backward looking. To help your insight, let us take a moment to look at the areas that regulators are turning their attention to. These are areas that will soon be, if they are not already, on the internal audit assurance radar.

The Fourth Industrial Revolution, also known as Industry 4.0 and related digital transformation is sweeping through all sectors and society as a whole. The speed of change and the complexities of the digital age alongside globalisation has been a challenging scenario for regulators, not just in the UK. Quantum technology, artificial intelligence, cryptocurrencies and cross-border data security are just some of the topics to address.

The Government recognises this and in May 2021 opened applications for a new £3m Regulators Pioneer Fund to help ensure regulators and local authorities keep pace with innovation, expanding funding beyond national bodies will enable innovation to be tested at a local level. The fund supports the 2019 White Paper, Regulation for the Fourth Industrial Revolution which outlines the roadmap for the UK.

Tech giants, Google and Facebook, face increasing pressure for regulatory censure from across the globe. The Online Safety Act, received Royal Assent in October 2023. Enforced by Ofcom, it includes the potential to impose substantial financial penalties (exceeding those under the GDPR), with fines up to the greater of £18 million, or 10% of global annual revenue.

Two of the FCAs five mid-term priorities also relate as they seek to make payments safe and accessible along with delivering fair value in a digital age. All against a backdrop of transformation and ensuring consumer protection amid post-pandemic economic challenges.

- In keeping with the theme of internal audit learning from regulators – what does 4.0 look like for your organisation and your internal audit function?
- Is digital governance embedded within decision-making?
- Is innovation informing strategy or causing chaos?

Regulation relevant to internal audit

Before we conclude, it is worth reflecting on the rigour of our own profession and the value that it brings for CAEs leading the internal audit activity:

- International Standards part of the International Professional Practices Framework (IPPF)
- Requirement for external quality assessment every five years (EQA)
- Requirement for an ongoing quality and improvement programme (QAIP)
- The Chartered IIA's Codes of Practice
    - Private and third sector
    - Financial services
- Public Sector Internal Audit Standards (PSIAS) based on the IPPF and issued by Chartered Institute of Public Finance and Accountancy (CIPFA).

Depending on sector, there are different regulators that are most relevant to the work of internal audit. Generally speaking, the Financial Reporting Council (FRC) is the most influential as its governance, risk management and internal control requirements for listed and large private companies are considered best practice across all sectors. Within its UK Corporate Governance Code there is a requirement for companies to have an internal audit function or explain its absence.

- Do you use these tools effectively?
- Are they fully embedded in your ways of working?

The FRC is undergoing transformation to become the Audit, Reporting and Governance Authority (ARGA), a tougher, more independent body with a much wider range of powers. Although the legislative timetable remains is unconfirmed. The future direction of the ARGA is a key element of the BEIS White Paper on Restoring Trust in Audit and Corporate Governance.

Conclusion

The similarities between the approach to right-touch regulation and internal audit clearly demonstrate the influence and value that internal auditors can bring to their organisation. Reflecting on the principles that underpin good assurance and the role of internal audit can be helpful in staying on track during periods of change. Next time you look at ways of working, pause to look at the big picture before ploughing into the detail.

"There can be no learning without action, and no action without learning."

Reg Revans, Professor and Management Consultant