

Q&A Extension



Chartered Institute of
Internal Auditors

**A journey towards excellence in
governance risk management,
and compliance (GRC)**

Marina McQuade

20 November 2020

Question 1

Bending policies to meet the solution, and integrating teams is a massive change for staff. How did you mitigate attrition and engagement risks?

Answer

We recognised the huge change impact and built effective change management plans into our programme. We sought to change people's experiences to feed their belief systems with the confidence that changes were necessary to achieve the integrated vision and that the changes were in line with our values. We established a centralised business support team and a network of user team administrators; and built strong governance and feedback mechanisms to ensure that there is buy-in, peer support (and pressure) and a growing momentum to come and join the transformation party. We also used our change managers to support the teams to build effective training plans that addressed both the system navigation and any changes to the process. As well as to document and file the final designs, test scripts, training packs, user manuals and admins guides with existing process documentation and mechanisms for review and upkeep. In particular, it was important that the training addressed both the onboarding of the current user population and how new hires in the future would be trained using the champion networks. Gaining leaders' understanding and support for what was necessary on the road ahead as well as upon immediate deployment was also key.



Question 2

Do diverse user groups present a challenge in maintaining the system?

Answer

Yes and that's why we established a centralised business support team within the Chief Risk Officer's organisation.



Question 3

Do you mandate specific risk wording (e.g. a staff attraction risk may be equally applicable to multiple service lines, with similar causes)?

Answer

No, but we have guardrails setting out guidance; communities of practise to hold ongoing training and dialogue about the ERM framework, etc. We also have harmonised language (remediations as opposed to actions); methodology (common repository means the same way of working with the system); rating scales (all findings are HML), etc.

Question 4

How do you obtain independent objective assurance about the adequacy and effectiveness of the GRC system?

Answer

We recently employed an external firm to review the programme and system's architecture to help guide our future direction. Their report was presented to the audit committee for consideration. I am quite sure that both our external auditors and any external firm could be employed to review this ongoing for any reason. Moreover, the recent review said our implementation was as good as any they have seen across their client base and this firm was a direct competitor of our implementation partner and experts in the GRC space!

Question 5

To clarify, would you recommend Archer over TeamMate? And, if so, would you recommend it for the second line of defence?

Answer

It depends. TeamMate is an excellent audit management tool, but RSA Archer is a different kind of tool - capable of the same functionalities as TeamMate for individual audit engagements and annual audit planning. But the beauty of Archer is it is an integrated GRC system, whereby the audit team can map their work to risks and controls in the risk and controls libraries, and, at the same time, have access to data from all first and second line teams to inform their ongoing planning and risk assessments. It is like comparing apples with a gourmet dish, made from all the ingredients of a greengrocery shop!

Question 6

Does all your reporting information come from Archer or do you use other solutions as well to produce MI?

Answer

We recognised early on the limitations from Archer in reporting and have implemented Power Bi dashboards to supplement Archer reports and dashboards.

Question 7

Do you have any guidance on how to effectively manage issues? Where does issue management sit?

Answer

Issue management is a shared application within the Archer system - we are moving to a situation in which findings are the outcomes of the risk, audit, assurance and compliance teams' work. But remediation is the accountability of the first line of defence teams. They are responsible for providing progress on updates, evidence of completion and stating that action is complete (with line manager review built into the workflows). But the second and third lines are accountable for closing the remediation plans once all are confirmed as completed to their satisfaction on review of the evidence.



Question 8

We use Galileo and I have used TeamMate. What is it about Archer that makes it better?

Answer

See my answer to Q5 - Archer does all that and meets the IIA's requirements. The richness of the data that leads to early warning and insights is on demand when needed.



Question 9

Is Archer integrated to the finance systems and does it provide real-time monitoring?

Answer

No. It is not. Archer is a lever arch folder in which sits the records of risks and controls. The finance system does the real-time monitoring and we are looking at how we can encompass that as a direct feed into Archer. However, it is a little way off as an integration on our roadmap.



Question 10

Do you manage action health and the trajectory of when you will expect a reduction in risk score?

Answer

Yes, we do. We are starting to get some traction, but this is quite new and we are at early maturity.



Question 11

With regard to value for money, is Archer comparable with the other systems in terms of cost?

Answer

I was not part of the team that purchased Archer and I cannot comment on its comparability to other systems in terms of cost. Each organisation has different needs.

Question 12

How did you manage to articulate the cost V benefit comparison to the board at the onset and during the process of the project?

Answer

We have seen some quantifiable benefits in terms of operational efficiencies in reporting e.g. month-end reporting for audit was a two-day production process that reduced to 15 mins. However, the real prize is the connections we can now make across the risk and compliance landscape to understand our hotspots and enable better decisions. It is the ability for an executive to see their business and the combined total impact of the work of all of the risk, assurance, audit and compliance teams on their risk profile and strategy - on demand, on one page/dashboard and the actionable strategies they can employ to head off issues bubbling up in a number of individual assurance and compliance lenses.

Question 13

One of the challenges is to manage a standard rating for audit observations - this cause issues. Could you share a key of how are you doing to keep this standard?

Answer

The audit team employ peer review to ensure their gradings are robust and agreed across the whole leadership. We have audit and risk business management standards as part of the National Grid book of standards and we are establishing co-ordinated assurance councils to provide strong governance alongside an Archer specific User Governance and Change committee.

Contact us



info@iia.org.uk



020 7498 0101

Follow us on



@CharteredIIA



Chartered Institute of Internal Auditors



@CharteredIIA

Our services

