ITM Head of Sales Matt Dodds

A new focus

Pensions Age speaks to Matt Dodds about the growing importance of ensuring good quality data

Data seems to be mentioned more and more in the pensions industry of late. Why is this and why is it happening now?
People are finally realising just how important data is – and that the consequences of ignoring it are just too severe. For years there has been a growing need to understand and control data and its quality, but over the past 18 months people have realised that data really is the ultimate enabler in all aspects of pensions. Whether it's paying people their benefits on time, complying with regulation, maintaining security, improving operational efficiency, providing dashboards or de-risking through liability management exercises, understanding what data you hold and its quality is essential.

Do you think attitudes towards data are changing within the industry?
I do, and there are many examples which is a real positive. We now know that dashboard will happen, the master trust market continues to develop and there is much talk at the moment about DB consolidation. Let's also not forget DC schemes, and the expensive and costly problems that data errors cause in that area, particularly with auto-enrolment increasing member numbers for years to come. I think the industry is realising that there is no escape from the reliance on data, wherever you turn, and whatever the aim, schemes are totally reliant on data integrity. One of the biggest shifts I have seen is that trustees and schemes are challenging administration teams on data quality. Common data scores are not a reasonable baseline – liability reduction, DB consolidation and compliance with the regulator are too important for schemes to think so narrowly. The landscape is evolving quickly, and schemes realise now that they have to modernise both their thinking and their practices or risk being left behind.

So there is a lot to think about and to be ready for. In what ways can schemes change their approach to ensure they don't get left behind?
We have to move away from the reactionary approach to data and think more strategically. In 2010 the regulator issued record keeping guidance, causing a largely reluctant reaction across the industry to 'tick the box'. Lots of work was done; then data moved back down the list of priorities. This effort profile of peaks and troughs simply doesn't work in today's landscape, there needs to be a concerted effort to improve data to enable schemes to meet wider objectives. GDPR takes effect in May 2018, cyber security is an increasing threat, DB schemes need to address growing deficits and DC schemes cannot contemplate compounding data errors – that's a lot of peaks, particularly when most schemes are already stretched. So we have to smooth the effort profile to keep on top of increasing demands and to allow schemes to achieve critical goals of de-risking, liability management and consolidation. The answer is to adopt a strategy for data; track progress against it, appoint a data-owner, and keep it on the agenda at trustee meetings in the same way that investment and governance already are.

What do you see as the major risks of failing to address data for pension schemes?
There are several – members expect accurate information to be available via a range of platforms – we risk further disengagement if we, as an industry, can't deliver this. Reputational damage caused by security breaches or other negative headlines can be hard to recover from. But the biggest risk, and the reason I see most schemes now adopting a data strategy and taking it seriously, is financial. The cost of not prioritising data is too great – both operationally with outdated approaches and lack of automation, but also at a strategic level. The upfront cost of understanding scheme data and making it work to your advantage is dwarfed by the financial implications of not being able to carry out that trivial commutation exercise, being unable to approach insurers when market conditions are favourable, or the risk premium applied if insurers believe data has not been audited and addressed.