Crowe

Smart decisions. Lasting value.

# Managing pension governance and risks effectively

## Risk Management Survey 2020

# Contents

# Introducing the fourth edition of the Governance and Risk Management report

As the nation moved into lockdown in March 2020, many service providers to pension schemes had to change their operations more rapidly than expected. Trustees had to get used to new ways of communicating, such as holding meetings virtually rather than in the more traditional boardroom. Scheme members thought more about what they could be doing with their pension pots, while fraudsters were thinking about how they could access their money and data. All these factors present challenges and now more than ever, Trustees need to make sure that they have strong governance and risk management practices in place to guide and protect their members.

Our fourth edition of the Governance and Risk Management report considers the changes to governance and operations of UK pension schemes in light of the effect of COVID-19 on working practices of pension schemes, both in the short and medium term.

The governance of pension schemes has not been a simple task since the first lockdown in March 2020. There has been a sudden need to reassess the strength of the employer's covenant and scheme funding levels, adjustments made to the controls and procedures by administrators due to remote working, and on top of this, an increase seen in fraud and cybercrime.

Now that there is light at the end of the tunnel with a vaccine, in this report we:

- reflect on how schemes responded to the initial impact of COVID-19 on their operational activities and strategic plans
- identify what Trustees need to consider going forward in light of any new working practices in place.

By now, Trustees will have received at least two quarterly administration reports and these would have been reviewed to identify what trends there have been in service levels. Where service levels have fallen, do Trustees know how these are being addressed going forward and are there available resources to enable the administrator to do this? Another key question for Trustees to consider, is do they know what changes have been made to the controls and procedures at their administrator and how this affects services to members?

Pension schemes are attractive to fraudsters. Large sums of money are being managed for beneficiaries, who, in most cases, have very little involvement in overseeing their accumulation, stretched over a long time period. Therefore, what assurances have Trustees received over this area?

Our benchmarking of scheme risks, for both Defined Benefit (DB) and Defined Contribution (DC), yielded some marked changes reflecting the increased awareness of cybercrime and fraud. It was also found that Trustees' attitudes to risk appetite and internal audit has changed, in comparison to 2019.

This report, based on 105 responses from Trustees of UK pension schemes, sets out the results of our survey. We will use this research to inform our conversations with clients as we help them to develop good governance and make smart decisions for their schemes that will have lasting value.

# Highlights

**28%**
of schemes do not utilise risk appetite.

**50%**
of schemes have not received assurance over fraud prevention procedures for member payments and vetting of staff.

**IT/Cyber**
is the top ranked risk for DB pension schemes.

**37%**
of Trustees are less confident in their administrator being able to deliver special projects since the start of 2020.

**25%**
of schemes do not have an adequate cybercrime breach plan.

**Inappropriate decisions**
made by members at retirement is the top ranked risk for DC pension schemes.

# Fraud and scams

In recent years, the pension liberation reforms have stimulated an increase in frauds targeting those with pensions. This has, in turn led to an increase in the action by authorities to tackle this problem. However, the media focus on ‘pension liberation frauds’ has masked a range of opportunities for fraud in the wider pension sector. These include frauds by those running pensions schemes, inappropriate investments and the targeting of pension schemes by external fraudsters, sometimes those involved in organised crime. These risks have received less attention.

Crowe’s research on The Nature and Extent of Pension Fraud, published in 2020, demonstrates the variety of fraud-types that can affect pension schemes. Over the past 12 months, there has been an overall increase of 4.3 million instances of fraud in the economy, which is partly due to the UK's current economic situation and this is not going to change overnight. Pension schemes are seen as attractive targets due to the high volume of payments made to members and the amount of personal data held.

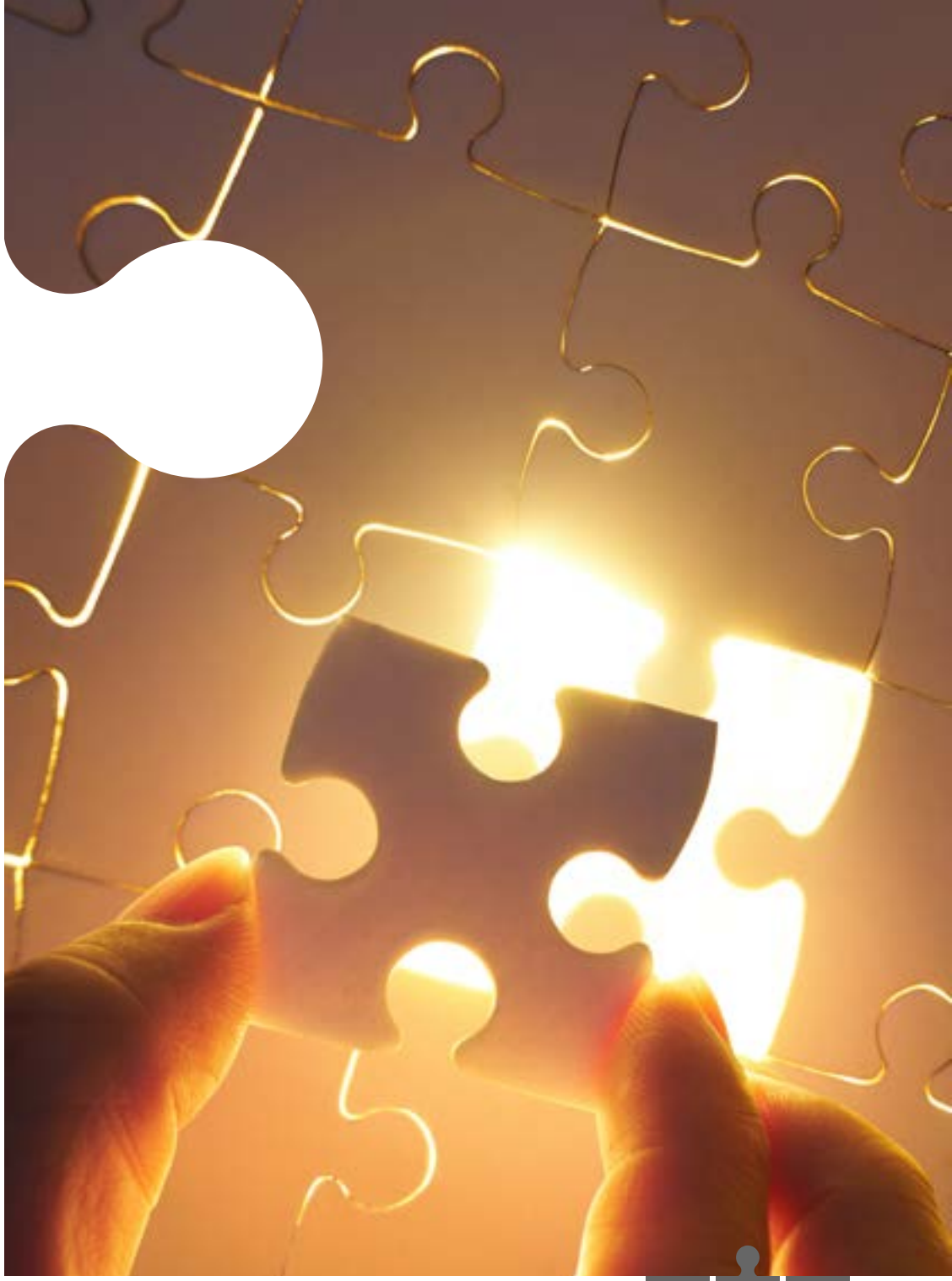


**Figure 1: Percentage of Trustees that have NOT undertaken an independent review of the member benefit payments processes**

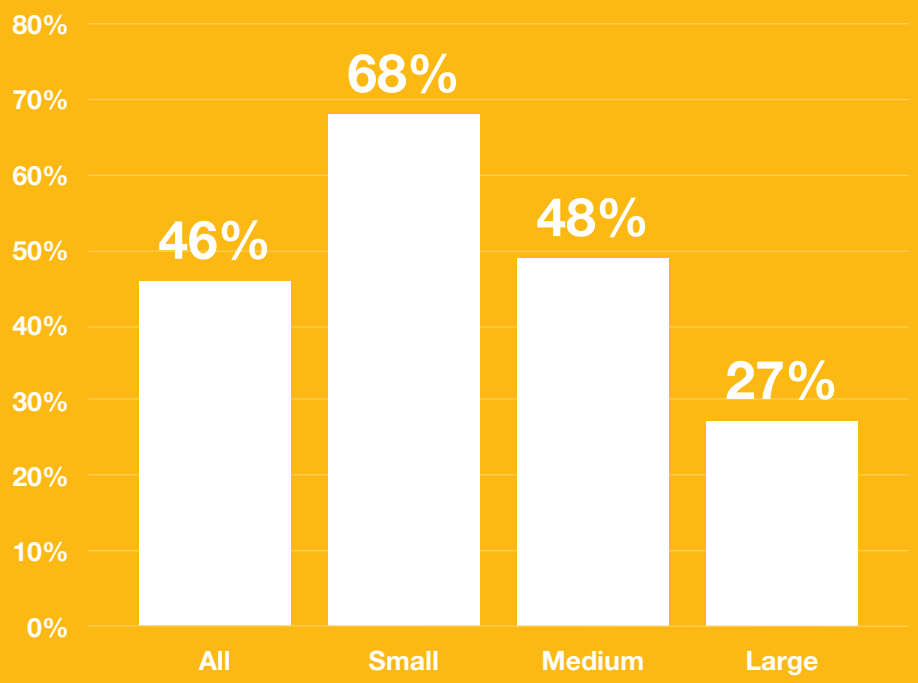



Figure 1 identifies what assurances Trustees have had over member benefit payments.

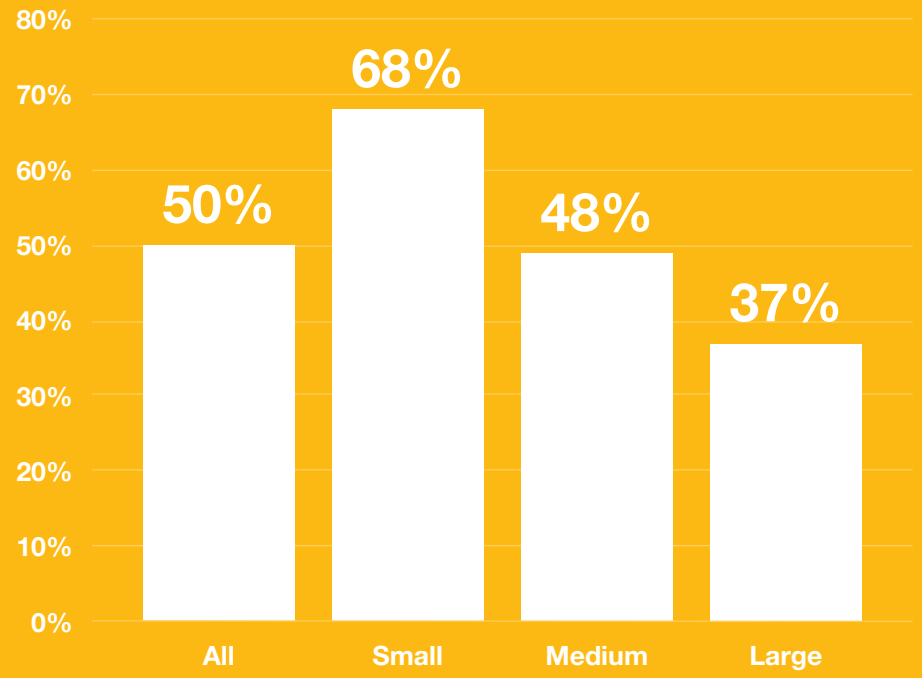
Almost half (46%) of all schemes have not undertaken an independent review of the processes for putting member benefits into payment. Such processes are targeted by fraudsters and are an important vulnerability that should not be left unchecked. In recent years, Crowe has seen numerous examples of administrators relying on old-fashioned identity verification methods that are highly vulnerable to fraud. The survey results show that the issue is more prevalent among small and medium schemes compared to large schemes.

The integrity of the people working for administrators is important in preventing fraud. Even with the right controls in place, dishonest people can often identify and exploit vulnerabilities. Pre-employment vetting, and more extensive background checks for employees in positions of responsibility, is an important process to strengthen fraud resilience.

As shown in figure 2, 50% of respondents have confirmed that their administrator has not had an independent review of its process for vetting staff with access to member data prior to their appointment, to ensure it is capable of preventing fraudsters gaining access to their systems and data. Again, there is a correlation with whether this has been confirmed based on the size of the scheme.

Irrespective of the size of the scheme it is important that Trustees understand what their administrators are doing to counter fraud, especially in the current climate of increased fraud risk.

**Figure 2: Percentage of schemes that have NOT undertaken an independent review of the process of vetting staff with access to member data**



# Cyber and information security

Fraud and cybercrime are identified as one of the top risks by Trustees of DB and DC schemes, as detailed later in the report.

**The survey asked whether Trustees had:**

**1**

Identified the key operations, IT systems and information flows vulnerable to cybercrime.

**2**

Assessed the vulnerability of their third party suppliers to cybercrime.

Figure 3 and 4 provide the survey responses for these two points for years 2020, 2019 and 2018.

The results suggest that despite considering cybercrime a top risk, many schemes are not doing enough to ensure they are managing cyber risks properly. 22% of all schemes have not identified the key operations, IT systems and information flows vulnerable to cybercrime, increasing to 28% of medium sized schemes. The results are similar for small schemes (24%) but less for large schemes (10%). Compared to previous years' results, there has been an increase in schemes that are unaware of their cybercrime vulnerabilities and unlikely to be managing cyber risks effectively.

The majority of what a pension scheme does is outsourced to third party providers, and as a result the majority of a scheme's cybercrime vulnerabilities will be outsourced too. The responsibility for managing cybercrime risks cannot be outsourced and remains a key part of Trustee obligations. Despite this, 29% of all schemes have not assessed the vulnerability of their third party suppliers to cybercrime. The figures range from 42% of small schemes, 36% of medium schemes, and 12% of large schemes. Almost a third of pension schemes have not identified cybercrime vulnerabilities posed by third party suppliers, and so cannot attain assurance that the risks are being managed appropriately. The figures seen for 2020 are higher than those seen in the 2019 Governance and Risk Management Report.

**These results are concerning, especially given that cybercrime has been ranked as the top risk for DB schemes in 2020 and is so prevalent at present.**

**Figure 3: Percentage of respondents that have NOT identified the key operations, IT systems and information flows vulnerable to cybercrime**

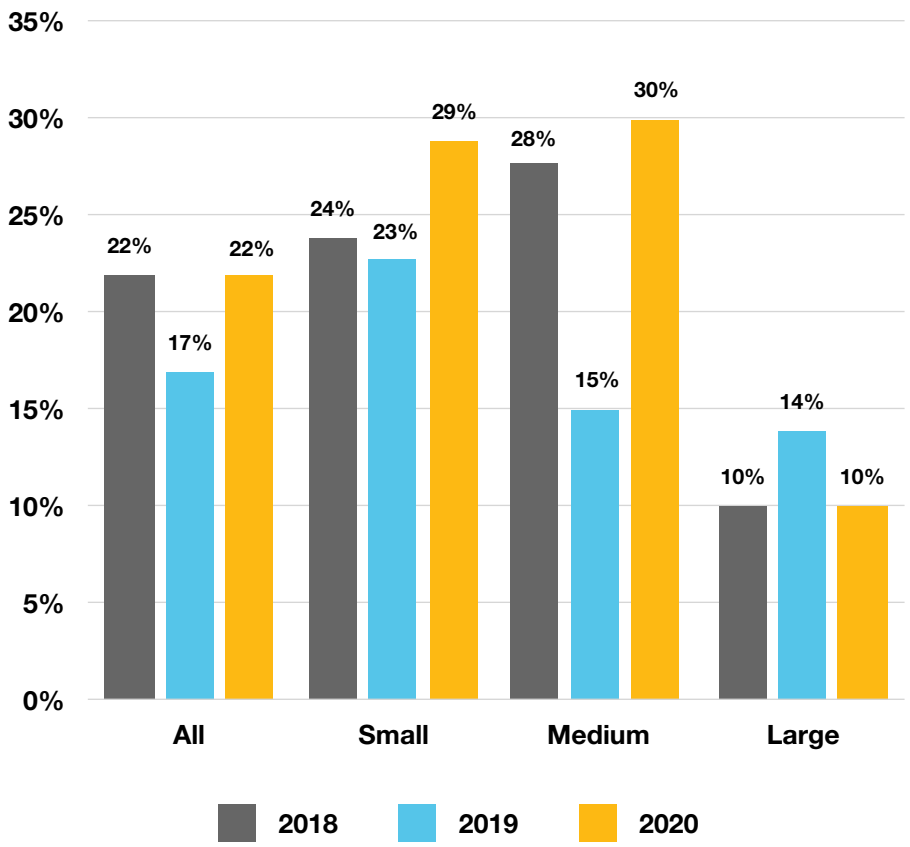
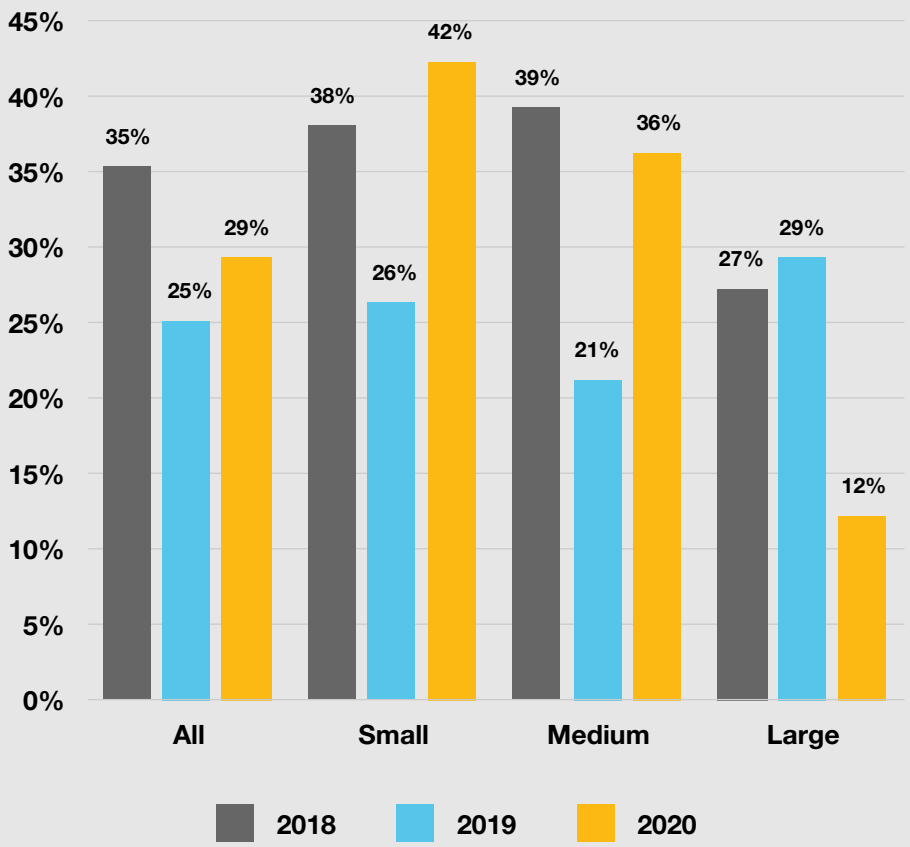



**Figure 4: Percentage of respondents that have NOT assessed the vulnerability of their third party suppliers to cybercrime**



## The survey asked respondents whether:

- they have access to the specialist skills needed to help investigate the nature of a cyber breach
- the Trustees received cybercrime scenario-based training.

Despite identifying cybercrime as a top risk, 42% of all schemes do not have access to specialist skills, and 59% have not provided cybercrime scenario-based training to Trustees (figure 5 and figure 6). The picture between schemes of different sizes is mixed, with large schemes tending to do better on both points due to the additional resources available to them.

**Figure 5: Percentage of respondents that do NOT have access to the specialist skills (not just generic IT skills) needed to investigate the nature of a cyber breach**

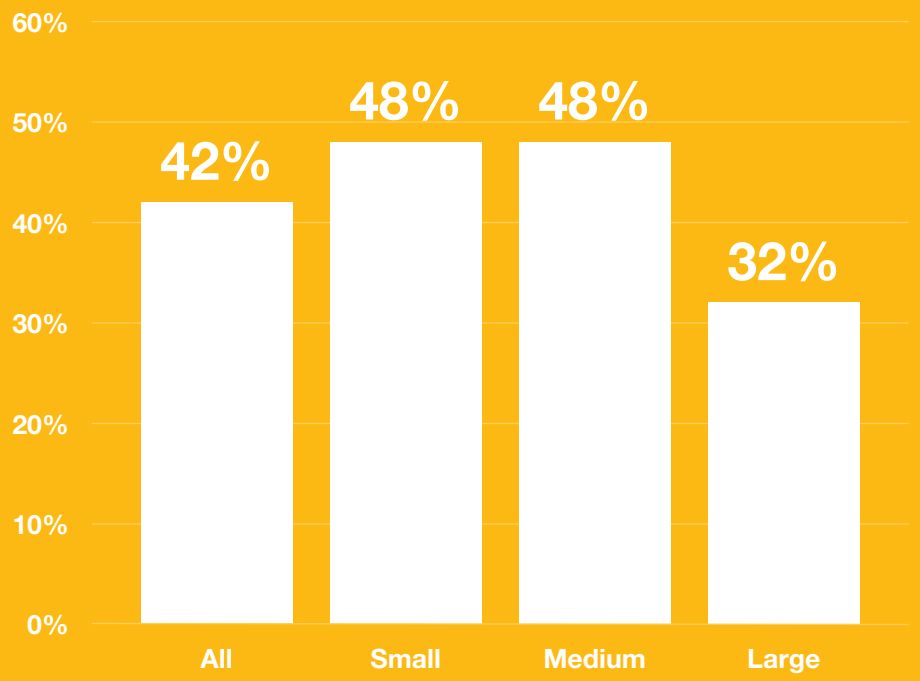
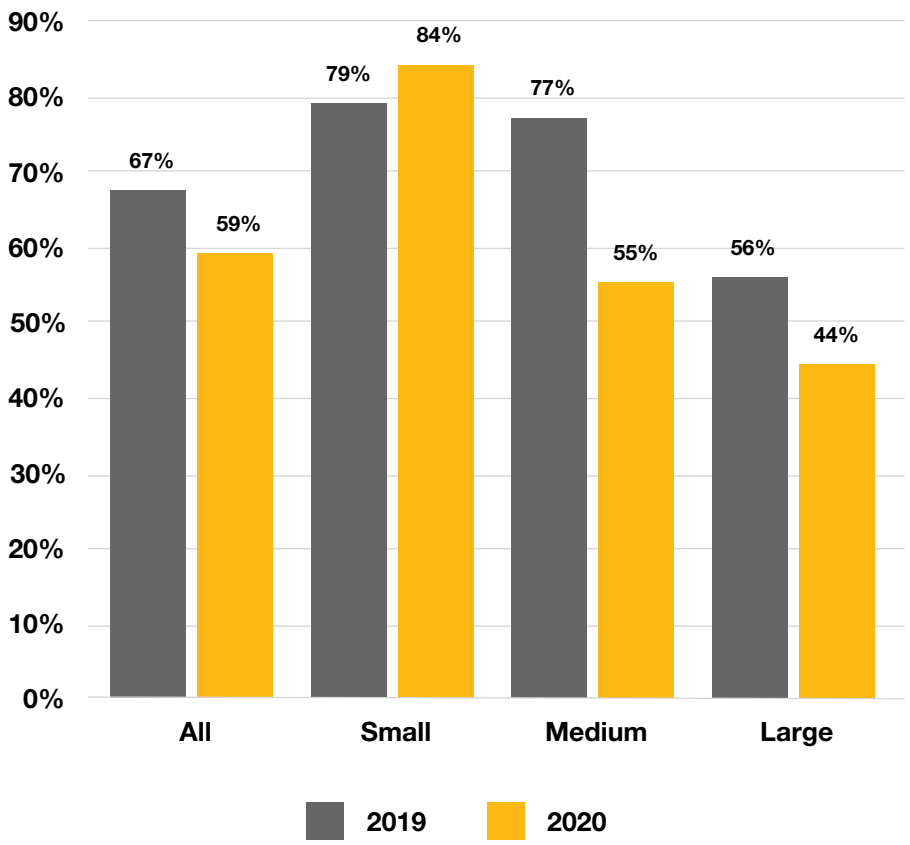


**Figure 6: Percentage of respondents that have NOT received cybercrime scenario-based training**



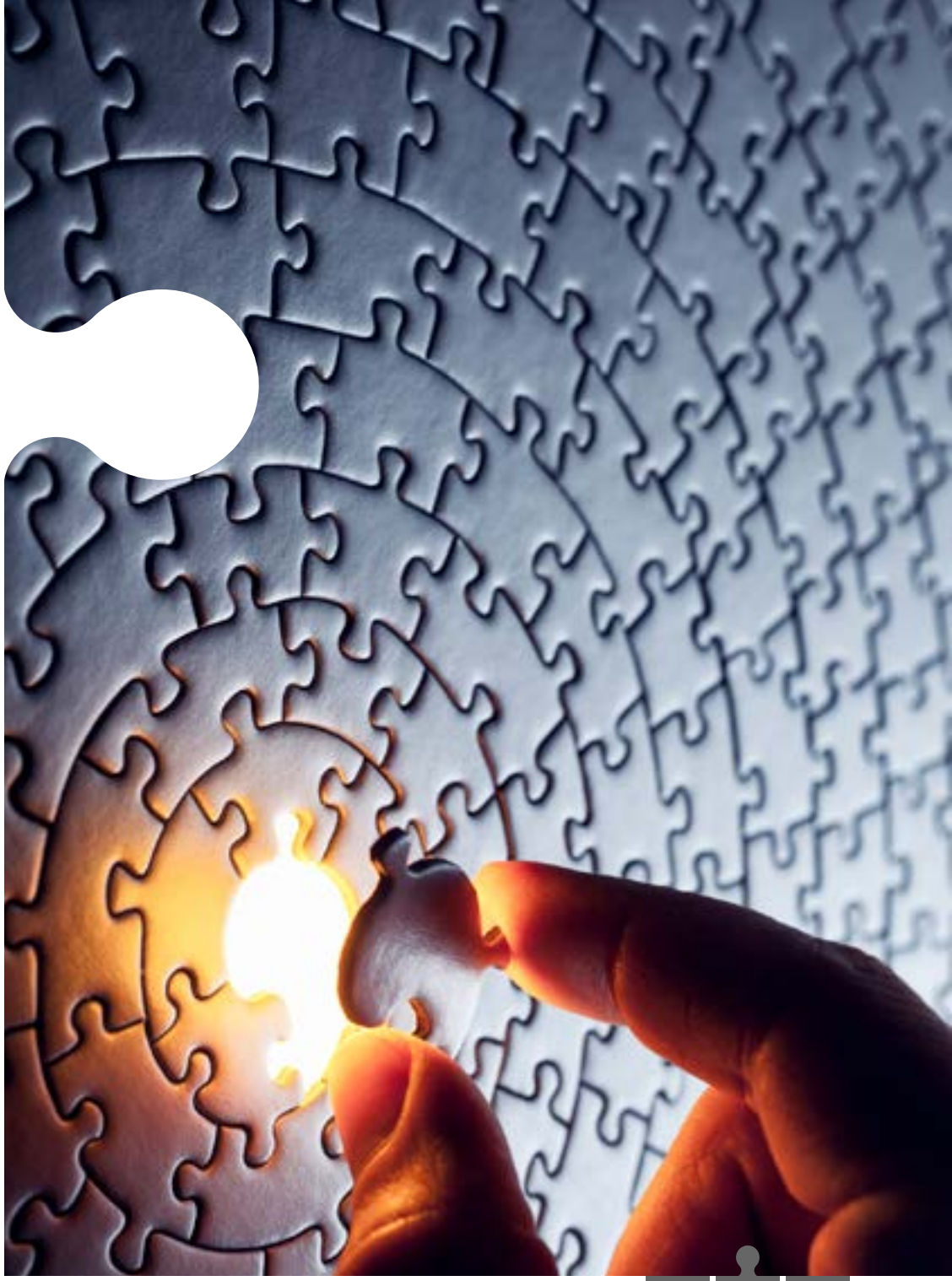
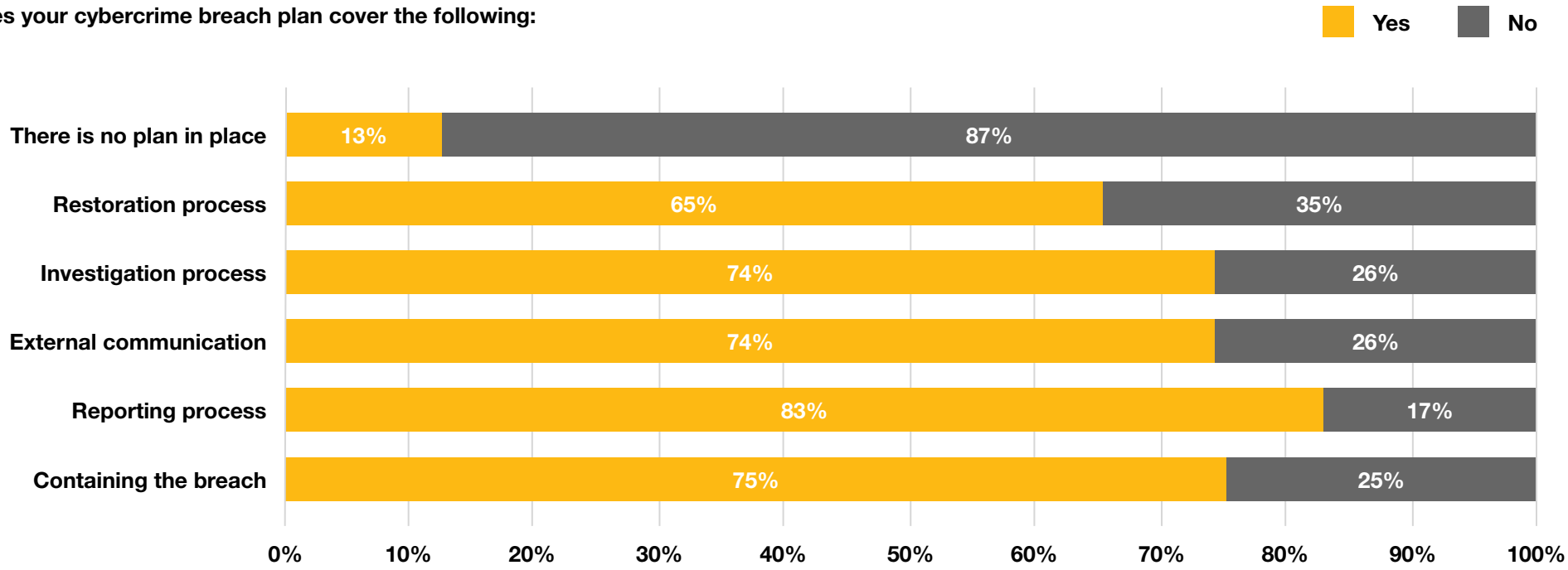



**Figure 7: Does your cybercrime breach plan cover the following:**



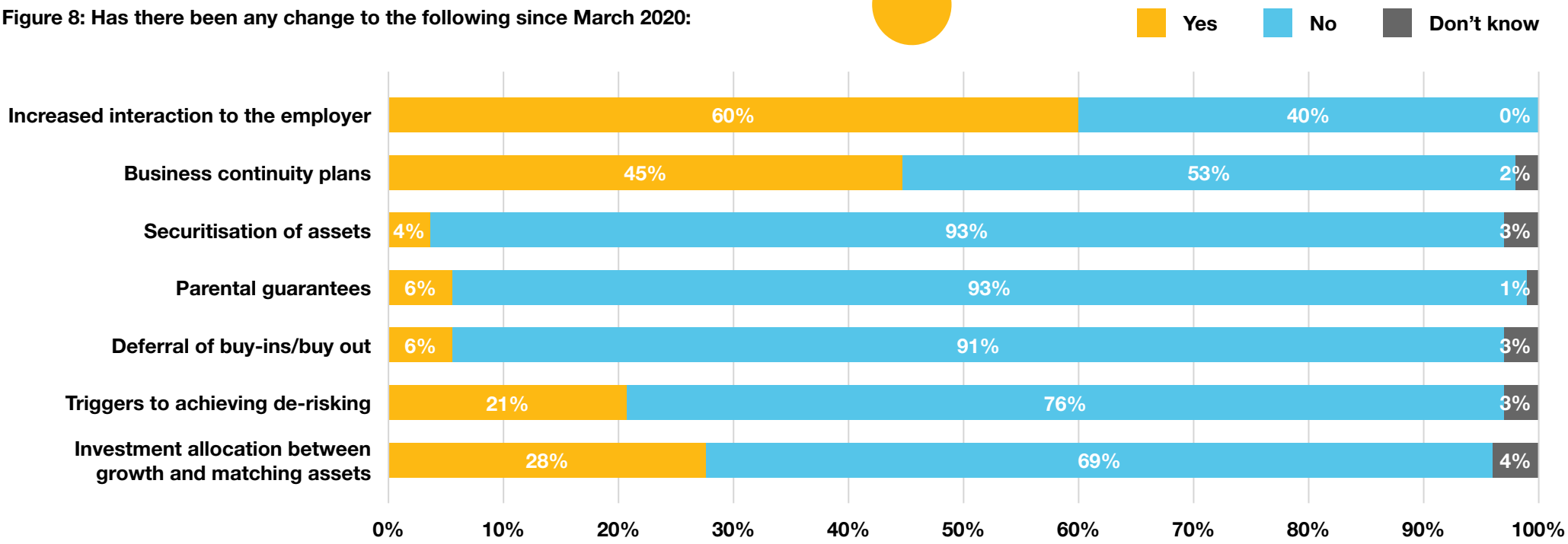

Fraud and cybercrime are the crimes of the 21st century, accounting for over half of all crime. Cybercrime alone has increased by 65% to the 12 months ending June 2019, and has increased even further since the COVID-19 related disruptions to the economy. Despite the prevalence of cybercrime and the potential impacts on pension schemes, over 10% of schemes do not have an incident response plan in place. Of those that do, around 25% have a plan without details of a restoration process, investigation process, external communications process, or details of how a breach would be contained should it happen (figure 7).

There is plenty of guidance available to assist Trustees in the preparation of a plan and Trustees, irrespective of scheme size, are encouraged to ensure they have a plan covering the items listed in figure 7.

# The impact of COVID-19 on pension schemes' strategic plans

When asked whether the pension scheme had a strategic plan in place, and whether there had been any changes since March 2020, 87% of total respondents confirmed that a strategic plan was in place, of which 87% of these schemes confirmed that there have been no changes to this plan. Given the long term nature of pension schemes, this response is not surprising. However, there have been a number of changes to some specific areas since March 2020, as detailed in figure 8:

**Figure 8: Has there been any change to the following since March 2020:**



Following the initial lockdown in March 2020, 60% of schemes increased their interaction with the employer and 45% of respondents confirmed there was a change to their business continuity plans. This result was expected given the shock to the economy and possible negative effect on the employer covenant, and also the potential changes to operations at advisors of pension schemes.

Over 90% of respondents confirmed that there has been no change to securitisation of assets or parental guarantees, which reflects the time it takes to put these types of arrangements in place.

Turning to investment allocations and triggers to achieve de-risking, it is encouraging to see that Trustees immediately considered the liability risk of their pension scheme in light of changes to the economy. 28% of respondents stated that they changed the allocation between growth and matching assets, and 21% adjusted the trigger levels.

# The pension schemes' administrator response to COVID-19

We asked respondents their views on their confidence in their administrator on delivering day-to-day activities and special projects (see figures 9 and 10).

**Figure 9: Percentage of Trustees confident that their administrator has the available resources to fulfil their scheme's day-to-day requirements**

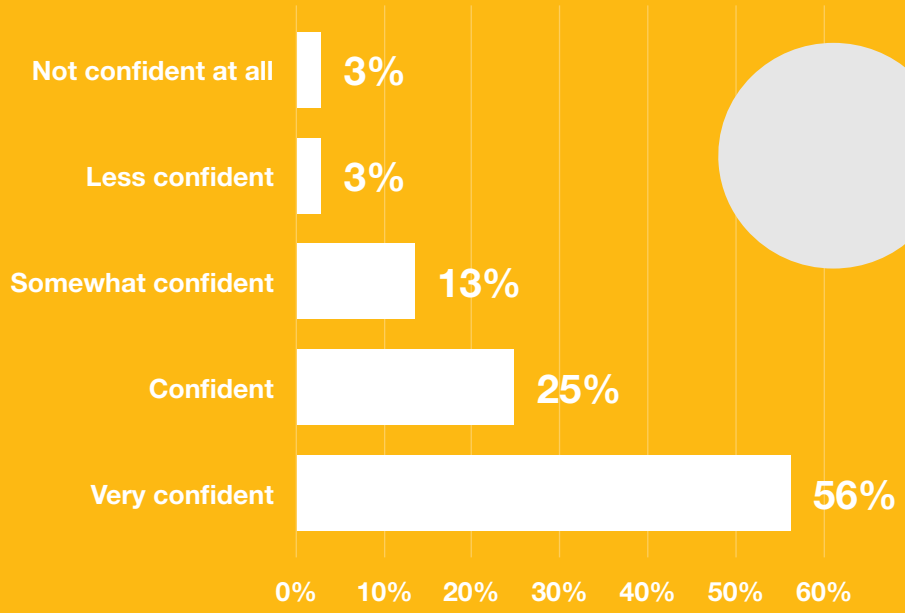
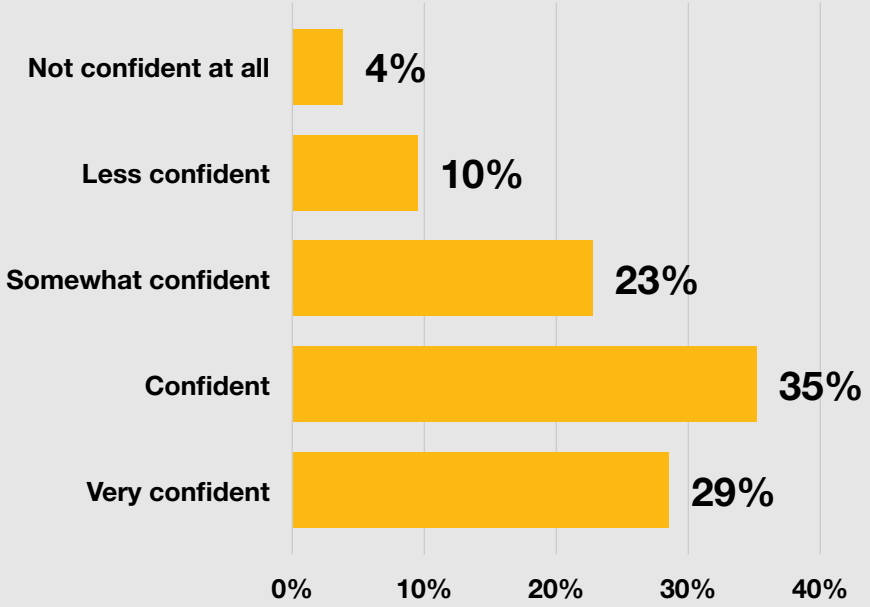



**Figure 10: Percentage of Trustees confident that their administrator has the available resources to fulfil their scheme's special projects**



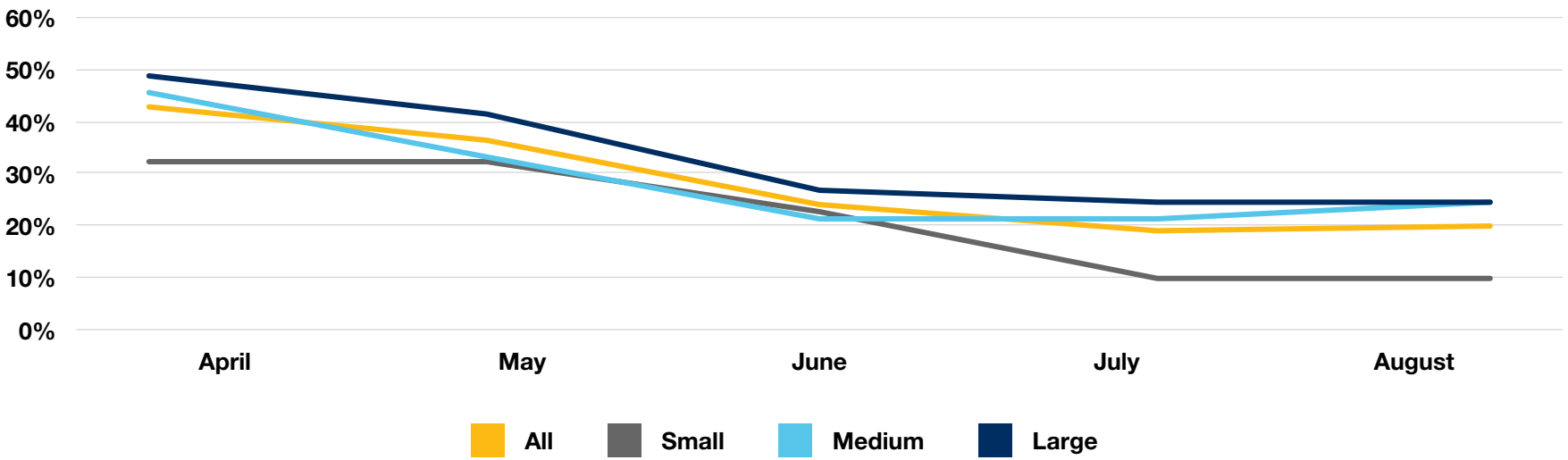
It was widely recognised in the pensions industry that the majority of administrators reacted swiftly to the lockdown in March 2020. This helped to ensure that business as usual activities remained unaffected as much as possible through careful planning and prioritising of activities, between the day-to-day activities and special project parts of their service to schemes.

It is encouraging to see that respondents continue to be confident in their administrator in delivering the scheme's day-to-day requirements, with only 6% of respondents stating that they are less or not confident at all that their administrator is delivering the necessary requirements.

Unsurprisingly, when turning to special projects, there is less confidence in the administrators having the available resource to deliver these. Trustees need to understand whether these special projects, such as data cleansing or Guaranteed Minimum Pension (GMP) rectification, are now critical to the operation of their scheme and if so, how the administrator will fulfil the requirements of the project and how this feeds into the strategic plan of the pension scheme.

When it comes to reviewing the service levels since March 2020, figure 11 shows an initial reduction in service levels, which is a reflection on the initial scramble to respond to the pandemic. This has reduced over time as organisations have become better adjusted to the new working practices. Interestingly the smaller the scheme, the less impact there has been on service levels, which reflects the lower levels of activities compared to the bigger schemes over the period.

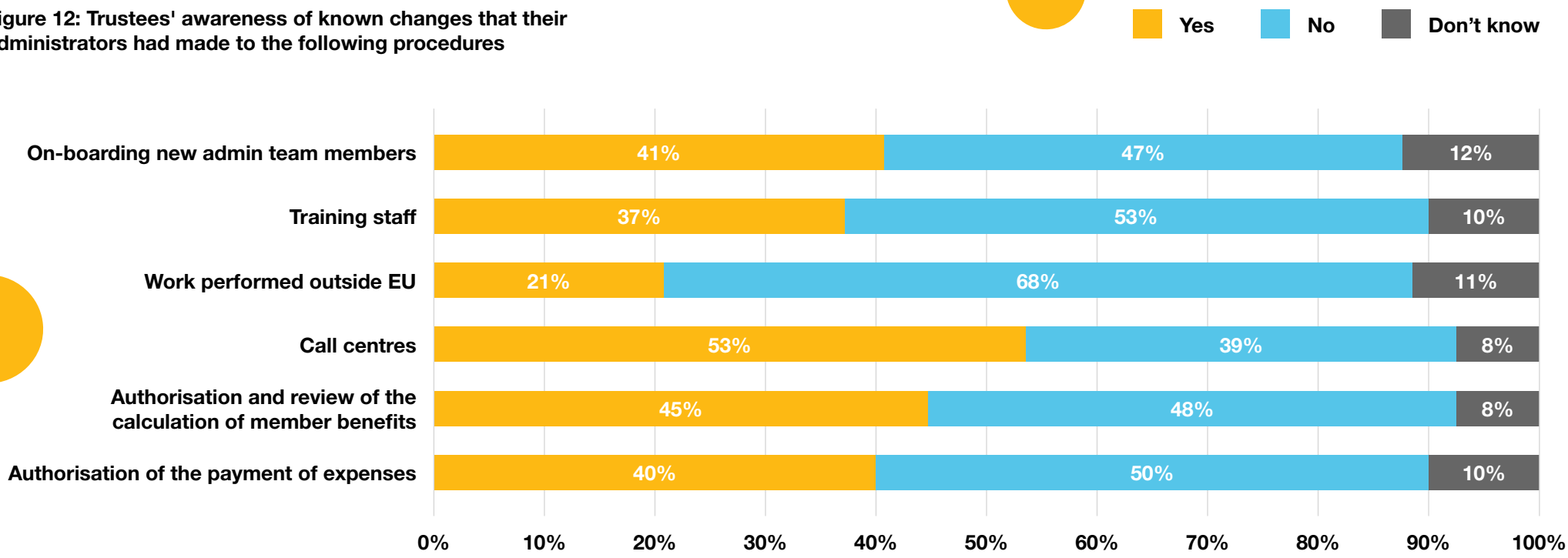
**Figure 11: Percentage of repondents that confirmed there was an impact on service levels since March 2020**



The UK's national lockdown and the ongoing restrictions on the public have had knock on consequences on the working practices of administrators. In figure 12 we asked respondents what known changes have occurred in some of the working practices of their administrator.

The results show an even split between changes and no changes to the procedures in place at the administrator. This may be because some administrators already had working practices in place to enable operations to occur through on-line systems. Trustees should consider how they can gain assurance over the changes that have occurred and, where the procedures haven't changed, are they still fit for purpose?

**Figure 12: Trustees' awareness of known changes that their administrators had made to the following procedures**



# Are Trustees still considering risk appetite and tolerance?

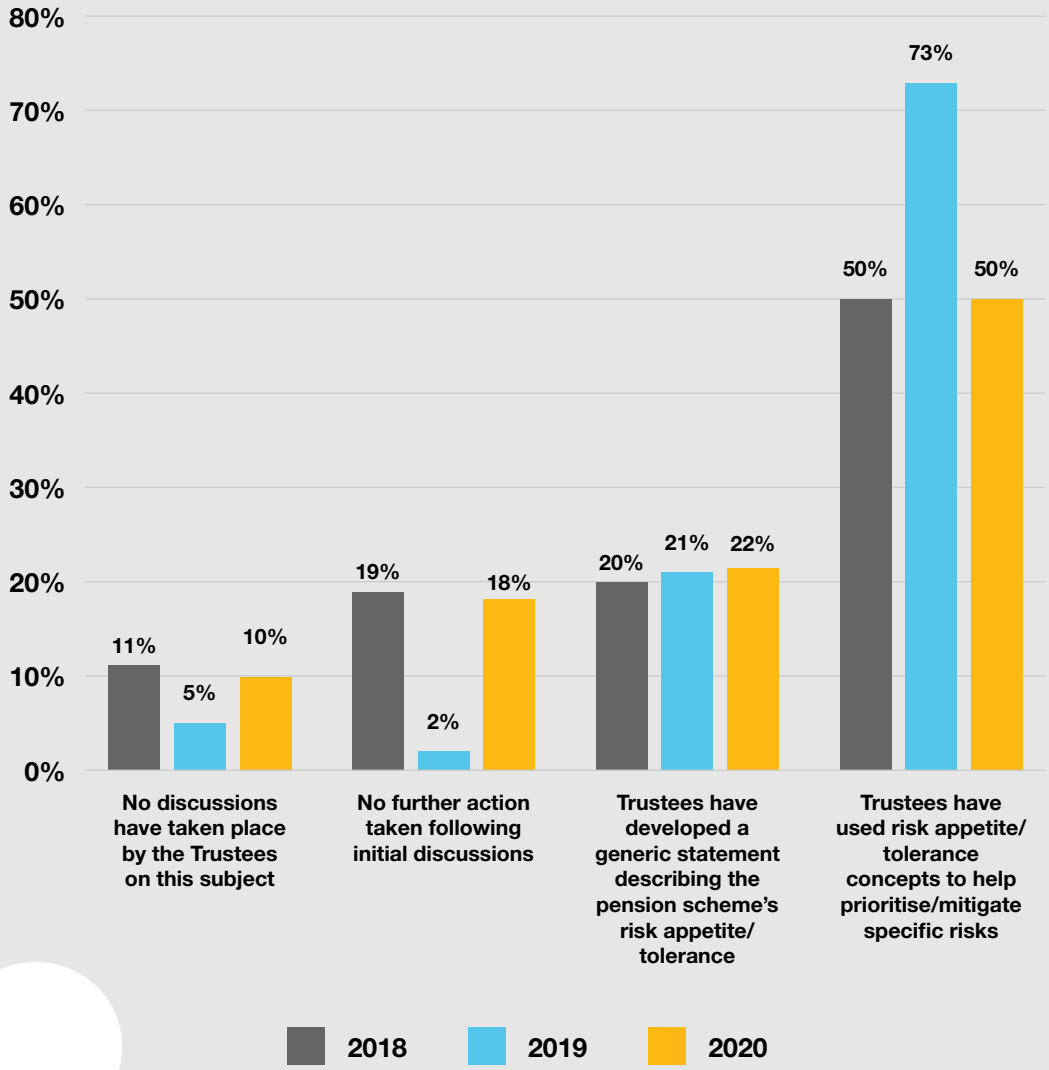
In 2018, the Pensions Regulator suggested that Trustees should consider their risk appetite and tolerance for risks, when determining potential risk prioritisation and mitigation techniques. We anticipate that this will be included in the Pensions Regulator's updated code of practice due in 2021 and therefore, we have summarised the movements over the last three years on the progress that Trustees have made in relation to this.

## Risk appetite/tolerance

- **Risk appetite** is the amount and type of risk that the pension scheme is willing to take in order to meet its strategic objectives.
- **Risk tolerance** is the amount of risk that a pension scheme can feasibly cope with.

It is disappointing to see that the results showed a move back to 2018 levels. This may have been due to the effect of COVID-19 on the scheme in 2020. In these riskier times, it is imperative to consider risk appetite and tolerance, as this method can assist in highlighting the areas for Trustees to focus on.

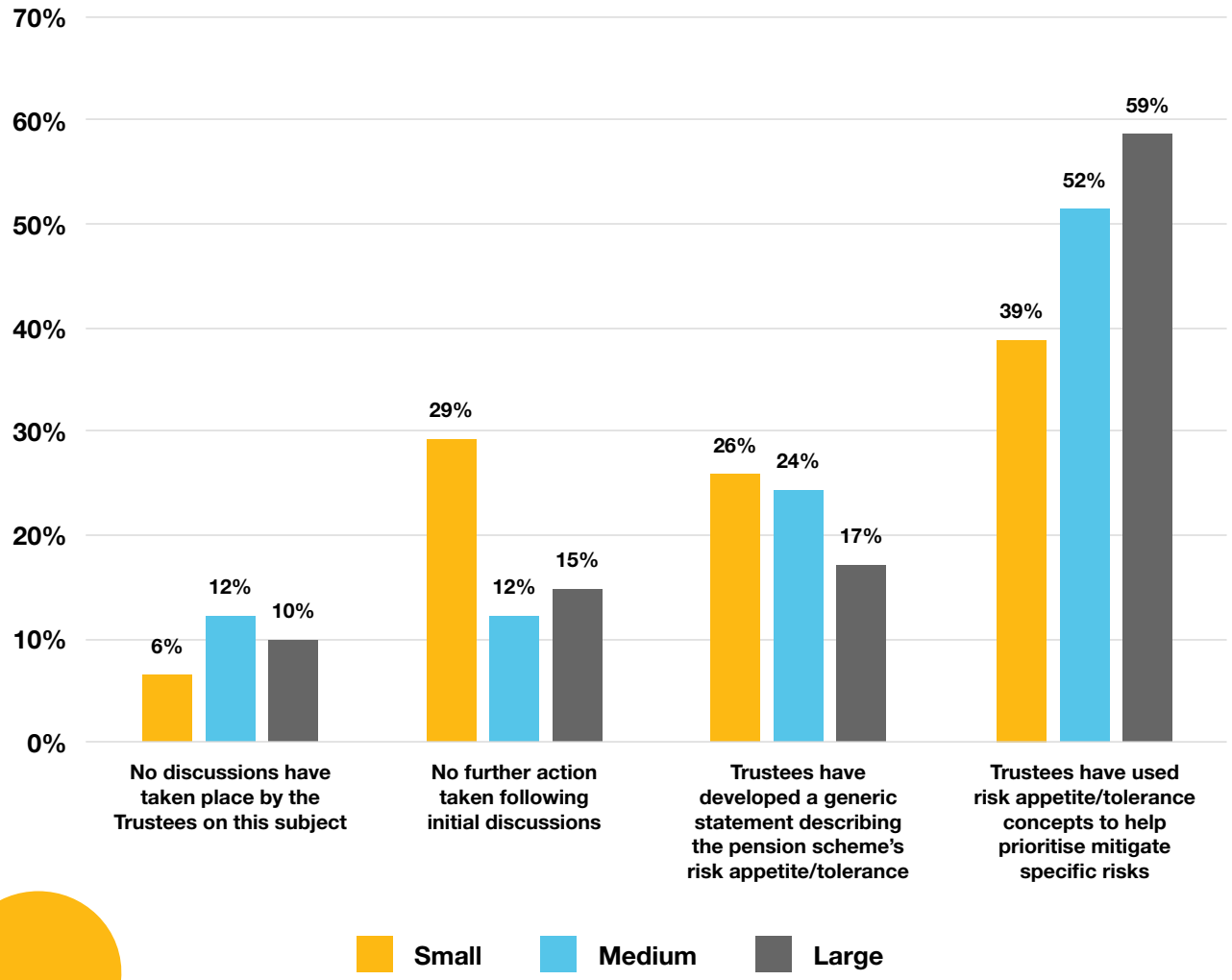
**Figure 13: Has your Trustee body discussed topics such as the Trustees' appetite or tolerance for risk?**



When analysing the responses between the sizes of scheme based on membership (see figure 14), there is an expected difference in using risk appetite/tolerance concepts between the larger schemes and smaller schemes. For smaller schemes, it would seem that this concept is either not considered worthwhile to pursue further, or a generic statement was put in place but these are not actually used in practice. This can either be put down to the limited resources available, or that the Trustees do not know how to use this tool effectively.

Trustees of all types of schemes should use these tools as this will highlight the areas that require more or less focus, which in turn would free up resources available to Trustees and create a framework to deal with emerging risks and unexpected opportunities.

**Figure 14: Has your Trustee body discussed topics such as the Trustees' appetite/tolerance for risk?**

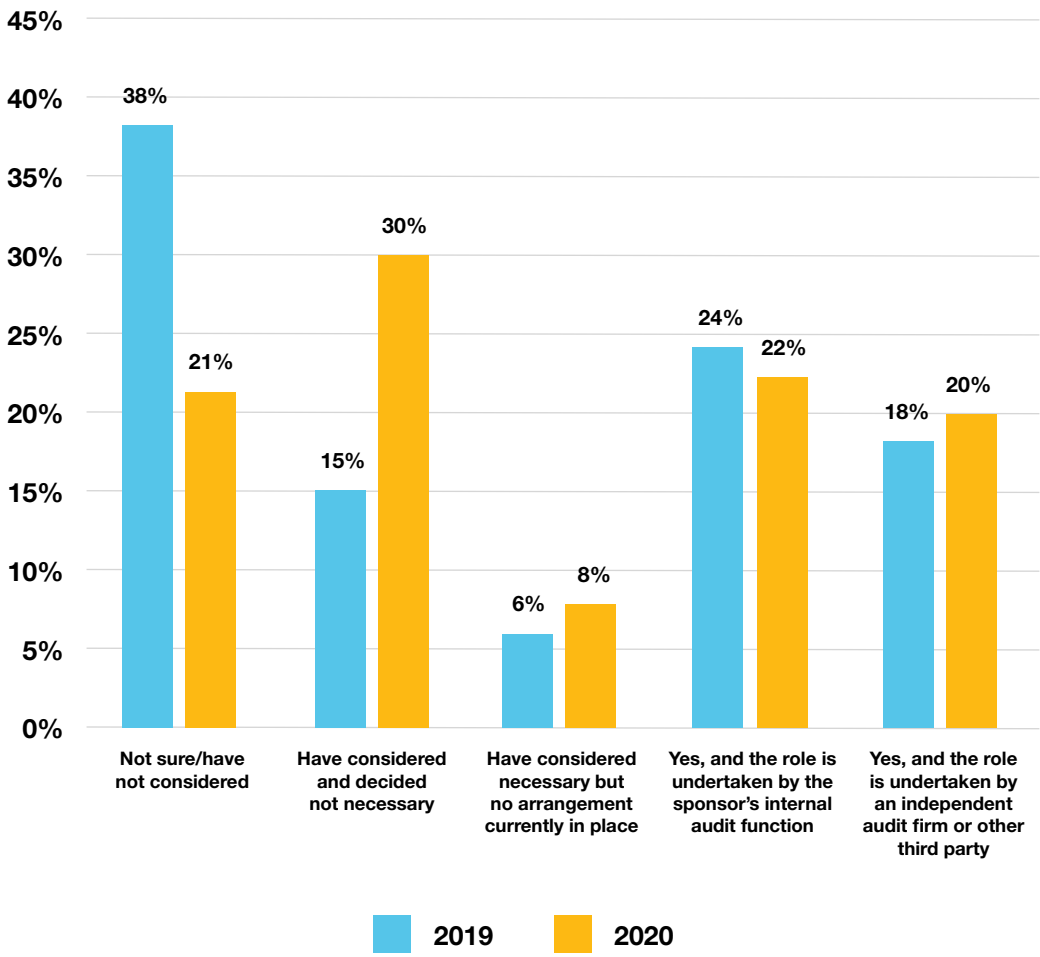


# Controls and procedures – how are these being verified?

The Pensions Regulator single code of practice, which is due for publication for comment in early 2021, may require an independent oversight for the assessment of scheme controls during a risk assessment. One of the methods to assess scheme controls is to appoint an internal auditor. When asking respondents on their views on who fulfils the role of internal auditor for their pension scheme, and how this compared to 2019 (see figure 15) we see a shift from schemes not considering internal audit to the decision that it is not considered necessary, and this was consistent across all sizes of schemes.

The challenge in the future will be how Trustees obtain assurance that the controls and procedures are operating as expected without the use of some sort of internal audit function.

**Figure 15: Respondents' views on who fulfils the role of internal auditor for their pension scheme**



# DB top pension risks trends

There has been a marked closure between all the risks that DB pension schemes are facing in light of the current circumstances with no one single risk being highlighted by our respondents. Although financial risks still dominate the top risks facing DB schemes, 'IT/Cyber risk' has come out as the most significant risk for DB pension schemes in 2020. This is not a surprise given the current climate and that pension schemes are an attractive target to cyber criminals.

Another risk that has increased in ranking has been ‘meeting regulatory/compliance requirements’ going from tenth to fourth largest risk. This reflects not only the increased regulation over the disclosure requirements covering investments such as ESG and data quality, but also ensuring that schemes continue to meet all the requirements following the changes to working practices due to COVID-19. It will be interesting to see what further requirements are needed following the publication of the Pensions Regulator combined code in early 2021 and how this changes this risk.

The ‘administration’ risk has dropped from fifth to outside the top 10 risks facing DB schemes. This was surprising given the changes to operations at administrators in 2020 due to the effects of the pandemic. However, as detailed earlier in this report, Trustees are confident that their administrators have the resources available to deliver the day-to-day requirements of their scheme and therefore other risks have overtaken the ‘administration’ risk in 2020.

# DC top pension risks trends

‘Inappropriate decision making by members at retirement’ has continued to be the top risk for DC schemes. This is not suprising in the current circumstances due to the uncertainty in the future and ever expanding options available to members that may not be suitable to the individual circumstances of that member.

Other trends include the rise in ‘IT/Cyber risk’ and ‘fraud/ scams’ to fourth and fifth on the list. Given the increased exposure of these types of threats in the press, seeing these risks move up in the ranks is hardly surprising. Trustees need to consider what controls and procedures are in place to mitigate these risks.

‘Poor communication’ and ‘investment performance monitoring’ have continued to fall down the ranking. This is consistent with the significant amount of work completed in 2018 over the DC Governance Statement. However, could Trustees consider how to use the communication already in place as a way to educate members on the decisions that they can make at retirement? Although they can not actively advise their members on what decisions to make, they may be able to provide more useful information and resources on where members can find independent financial advice.

# In conclusion

2020 was a year of challenges for Trustees following the impact of COVID-19. It is clear that a significant amount of work has been completed to ensure the operations of pension schemes remained unaffected. However, with the increased risk of cybercrime and fraud together with changes to working practices over the last year, here are six key questions that Trustees should be asking.

1. What are your administrators doing to counter fraud, especially in the process of putting members' benefits into payment and how they vet new staff with access to member data?
2. Are you aware of your cybercrime vulnerabilities and how cyber risks are being managed?
3. Does your cybercrime breach plan include all the areas it needs to as detailed in the cybercrime and information security section?
4. How do you utilise risk appetite/tolerance tools to create a framework to deal with emerging risks and unexpected opportunities?
5. Have you assessed if the systems, controls and processes at the administrator are still fit for purpose due to remote working?
6. Given the decrease in the use of independent oversight for the assessment of scheme controls, how has assurance been obtained to confirm that they are operating as expected?

# How Crowe can support you

## Fraud

A pension scheme's third party suppliers include those who undertake member administration, pensions payroll, banking and asset management, payment processing, insurance including buy-ins, accounting, actuarial, legal and other support services. Many will hold or have access to sensitive personal data, commercial data and have payment/asset transfer capabilities.

We can help clients to implement an action plan to ensure that the pension scheme has the controls and procedures in place to minimise the threat posed from fraud.

Where a fraud or other financial loss through dishonesty occurs, we can discover what has happened, identify those responsible, prevent further loss (financial and reputational) and recover what has been taken.

## Cybercrime

We assess the vulnerability of pension organisations to cybercrime, to highlight strengths and weaknesses in protection and, to recommend any necessary improvements. Our cybercrime vulnerability review works with Trustees to consider:

- governance and data security policies
- data systems including ownership, accessibility and behaviours
- protections in place including cyber essentials plus
- preparations to respond to cybercrime
- plans to recover from a cybercrime attack.

We work with pension scheme Trustees and their advisors to help them better understand the full effects of cybercrime.

## Trustee effectiveness

The success of pension schemes in providing the best possible outcomes for members will be enhanced by an effective Trustee Board.

We invest the time to understand what skills, expertise, experience and personalities are on the Trustee Board, to enable us to provide you with constructive feedback so that you can drive the scheme forward to meet its objectives.

We also ensure we understand your structures and processes which support your decision making.

## Internal audit/assurance

Our internal audit approach is delivered through co-sourcing, outsourcing or a combination of these approaches.

Our pensions internal audit service provides assurance that appropriate policies, procedures and controls are in place to mitigate key pension scheme risks as part of good scheme governance and supports the latest '21st Century Trusteeship' initiative and Codes of Practice issued by the Pensions Regulator.

## Risk assessment

With the expanding regulatory requirements on Trustees to take ownership of risk management of their schemes, having good systems in place is vital to ensure compliance.

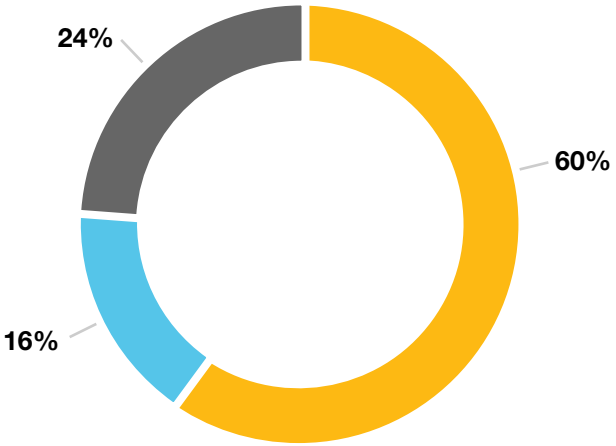
We help and support Trustees by evaluating pension scheme governance arrangements, including risk management, policies and practices.

This will lead to good decision making and good member outcomes.

# Appendix: summary of participants

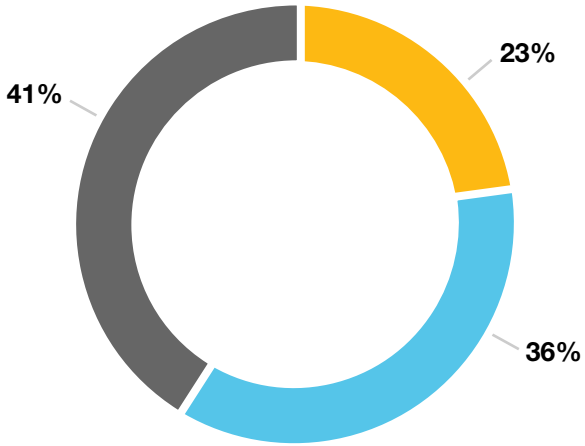
In total, we had 105 responses to our survey, covering a broad range of occupational Trust based pension schemes in the UK. The breakdown by type of pension scheme, size by net assets and members can be found below.

## Type of pension arrangement



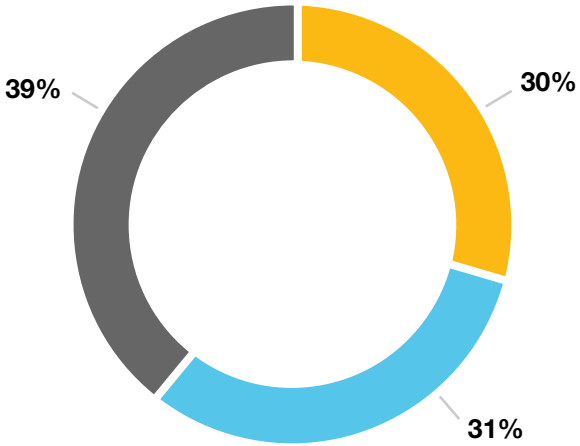

- Trust based DB
- Trust based DC
- Hybrid (i.e. both DB and DC)

## Size of pension arrangement




- Less than £100m assets
- £100m-£1,000 assets
- more than £1,000m assets

## Membership size




- Less than 1,000 members
- 1,000-9,999 members
- more than 10,000 members

## Start the conversation

**Andrew Penketh**
National Head of Pension Funds
London
andrew.penketh@crowe.co.uk
+44 (0)20 7842 7355

**Judith Hetherington**
Partner
London and Midlands
judith.hetherington@crowe.co.uk
+44 (0)20 7842 7324

**Shona Harvie**
Partner
London and Thames Valley
shona.harvie@crowe.co.uk
+44 (0)20 7842 7105

**Michael Jayson**
Partner
Manchester
michael.jayson@crowe.co.uk
+44 (0)161 214 7520

@CroweUK

www.crowe.co.uk

# About Us

Crowe UK is a national audit, tax, advisory and risk firm with global reach and local expertise. We are an independent member of Crowe Global, the eighth largest accounting network in the world. With exceptional knowledge of the business environment, our professionals share one commitment, to deliver excellence.

We are trusted by thousands of clients for our specialist advice, our ability to make smart decisions and our readiness to provide lasting value. Our broad technical expertise and deep market knowledge means we are well placed to offer insight and pragmatic advice to all the organisations and individuals with whom we work. Close working relationships are at the heart of our effective service delivery.