

# How protected are your schemes against fraud and cybercrime?

Risk Management  
Survey 2021



# Contents

- 3 [Introduction](#)
- 6 [Highlights](#)
- 7 [Fraud – Electronic verification](#)
- 9 [Fraud – Pensioner existence checks](#)
- 10 [Fraud – Independent review of processes](#)
- 12 [Cyber and information security](#)
- 15 [Cybercrime protection – policies](#)
- 16 [Cybercrime protection – cyber incident response plan](#)
- 17 [Cybercrime protection – investigation, training and insurance](#)
- 19 [Defined Benefit \(DB\) top pension risks trends](#)
- 21 [Defined Contribution \(DC\) top pension risks trends](#)
- 23 [Conclusion](#)
- 24 [How Crowe can support you](#)
- 25 [Appendix: Summary of participants](#)
- 26 [Start the conversation](#)



# Introducing the **fifth** edition of the Governance and Risk Management report

The latest Office for National Statistics (ONS) figures for the number of incidents of cybercrime show that in the 12 months ended September 2021, there were 1,869,000 incidents of cybercrime in England and Wales compared to 876,000 in the same period prior to March 2020; an increase of 113%. Incidents of fraud have increased by 39% in the same period.

In the period after April 2020, the number of cyber breaches reported by pension schemes to the Information Commissioner's Office (ICO) rose from an average of two per month to five per month. 35 pension schemes reported 39 cyber breaches in an eight-month period. Figures for the subsequent period are not yet available but, given the wider picture, it is unlikely that the position has improved.

## Types of fraud reported

- Internal frauds by those administering pensions schemes such as manipulation of records to enable pensioners to receive a pension they are not entitled to or diversion of payments from legitimate pensioners.
- Opportunistic pension fraud, for example close relatives of a deceased person who fail to declare their death or falsify details enabling benefits to continue to be claimed.
- Investment and misappropriation risks such as corrupt insiders investing in inappropriate schemes and organised fraudsters targeting staff running pension funds.
- Impersonation of legitimate beneficiaries to divert payments.





Therefore, Trustees should be asking important questions, such as:

- what form of verification does your administrator use prior to the payment of member events?
- how frequently do pensioner existence checks occur?
- what controls and processes does your administrator have in place to update member data such as changes to bank details and addresses?

The ICO cyber breach data for pension schemes shows the attacks split between those involving ransomware (56%), phishing (28%) and other types of unauthorised access (16%).

To properly exercise their governance responsibilities in this respect, Trustees need to:

- assess and understand how cyber resilient they and their third-party suppliers are
- arrange for revealed vulnerabilities to be removed
- establish a Cyber Incident Response policy to ensure an effective response when (if) an attack takes place.







Despite the prevalence of cybercrime and the potential impact on pension schemes, we reported in our 2020 Risk Management Report over 10% of respondents do not have an incident response plan in place. Of those that do, only 25% have a plan without details of a restoration process, investigation process, external communications process, or details of how a breach would be contained. There is plenty of guidance available to assist Trustees in the preparation of a plan and we encourage Trustees, irrespective of scheme size, to ensure they have a plan covering these types of items.

Our 2021 Governance and Risk Management survey looks at the progress that has been made over the last year on:

- how confident the Trustees of pension schemes are that they have the right processes in place to protect against fraud and cybercrime
- if there is a breach, are there procedures in place to react.

Our benchmarking of scheme risks, both for 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 the last three years.

This report, based on 93 responses from Trustees of UK pension schemes, sets out the results of our survey. Where we have analysed the results between the size of the schemes, we have based this on membership numbers.

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

**29%** and **63%**

of schemes **do not** use member electronic ID verification for UK and overseas members respectively.

**Not all schemes**

have a policy covering the data requirements and how this is transferred securely to their suppliers.

**IT/Cyber**

is in the **top two ranked risks** for DB and DC pension schemes.

**43%**

of respondents **have not tested** the strength of their scheme's IT systems, processes and procedures for cybercrime protection.

**28%**

of respondents **have not assessed** the vulnerability of their third-party suppliers to cybercrime.



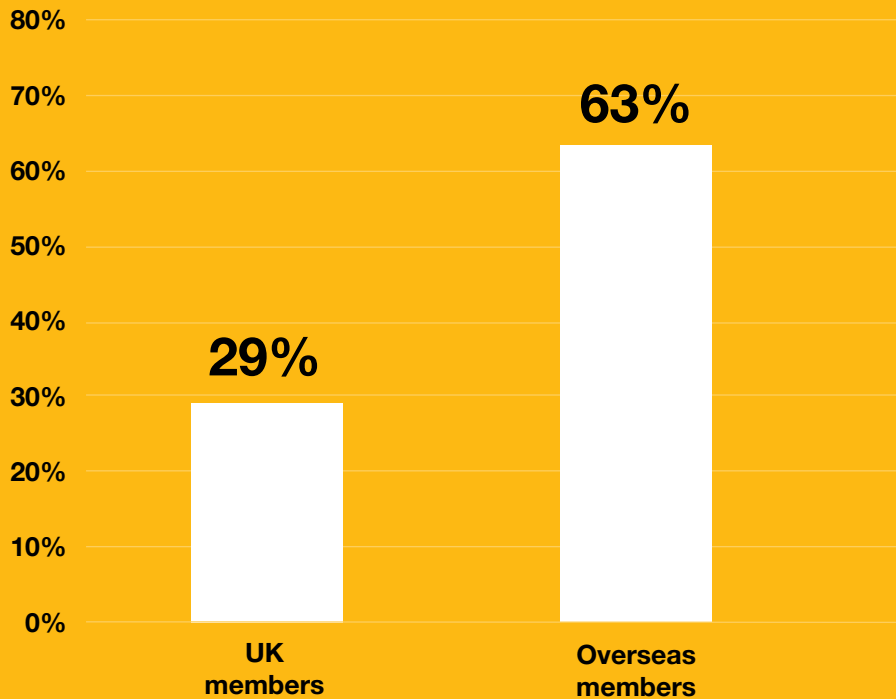
# Fraud – electronic verification

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 pensions 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.

One fraud area that is targeted by fraudsters both external, and internal to the pension scheme is member identity theft. Over the past few years, we have identified an increase in the use of an electronic system for ID verification by pension scheme administrators as part of member event processes. Figure 1 identifies whether pension scheme administrators use an electronic system for ID verification for UK and overseas members.



**Figure 1: Percentage of respondents that confirmed that their administrator does not use an electronic system for ID verification for the following type of members:**



It is surprising that 29% of respondents confirmed that there is no electronic ID verification for UK members. From our experience the majority of administrators have such an ID verification system in place for UK members, therefore Trustees should consider requesting this from their administrators as part of their normal service to their pension scheme.

Electronic ID verification methods for overseas members has always been behind any system for UK members, but from the answers provided 37% confirmed that they currently have use of such tools. Trustees should request from their administrators information concerning what system they have, and if there is no system currently in place what plans do they have in the future to put these tools in place.



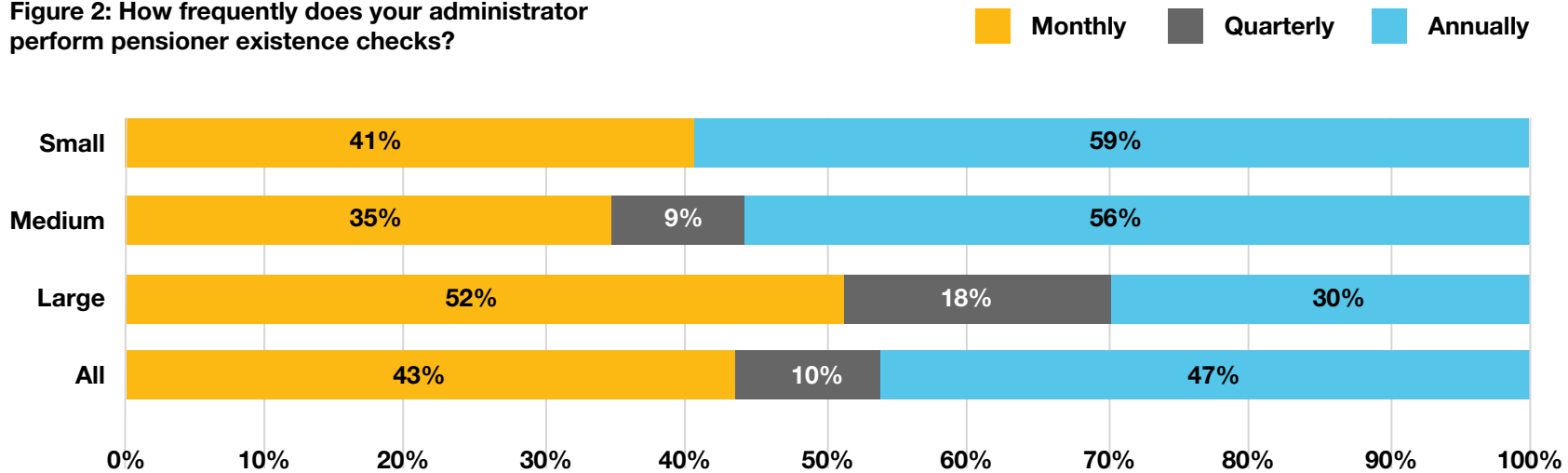


# Fraud – pensioner existence checks

One of the frauds that has occurred in pension schemes for many years is claiming pension payments following the death of the pensioner. Over the years, pensioner existence checks have become more commonplace to ensure that pension payments are stopped where applicable. Figure 2 shows the frequency of when pensioner existence checks are being completed.

The results show that the smaller the pension scheme, the less frequent existence checks are completed. We are aware that frauds still occur in this area, so consideration should be made on whether these checks should be performed more frequently.

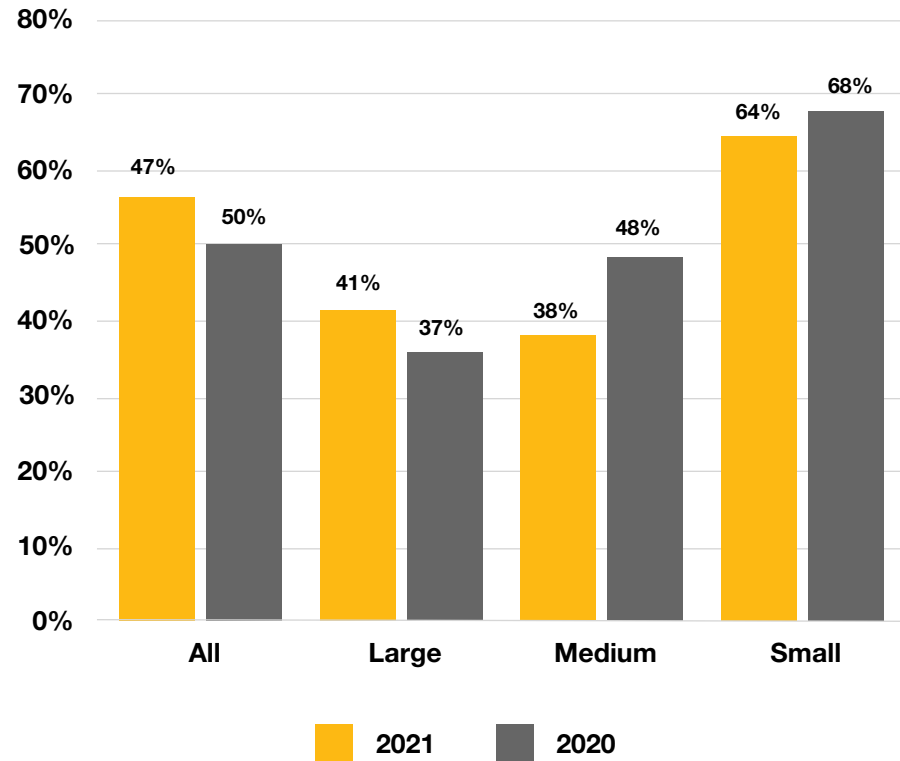
Figure 2: How frequently does your administrator perform pensioner existence checks?



# Fraud – independent review of processes

Over the past 12 months, there has been an overall increase in 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 and aggregate value of payments made to members and the amount of personal data held.

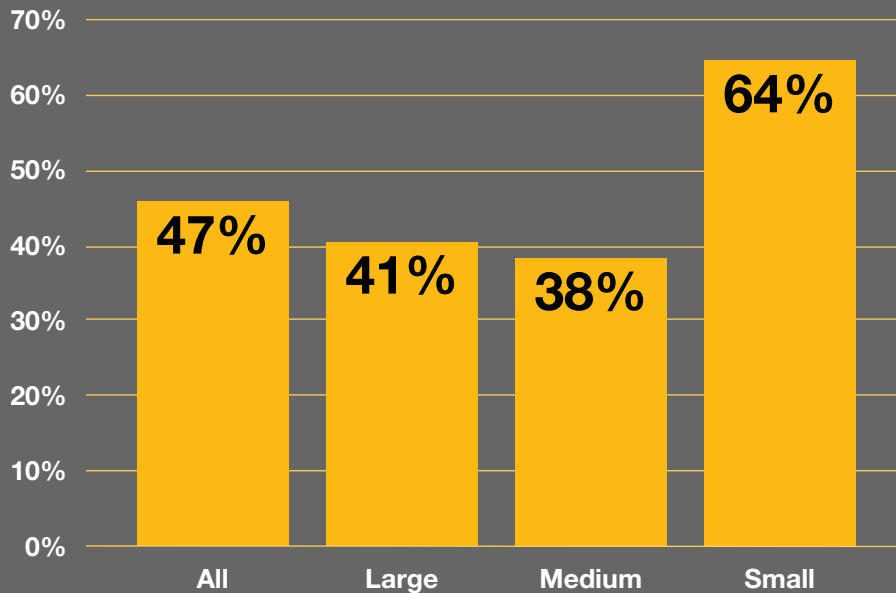
Figure 3: Percentage of schemes that have not had an independent review of the process of vetting staff with access to member data



The integrity of the people working for administrators is an important factor in preventing fraud. Even with appropriate controls in place, the minority of 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 3, 47% 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.



**Figure 4: Percentage of schemes that have not had an independent review of its process for updating member details when informed of a data change e.g. address, bank details?**



Almost half (47%) of all schemes have not undertaken an independent review of the processes their administrator has in place for updating member details, when informed of a data change. Such processes are targeted by fraudsters and are an important vulnerability that should not be left unchecked. In recent years, Crowe has seen examples of fraudsters using false information to change member details. Therefore, it is fundamental that Trustees have assurance that the processes in place are effective. The results show that no independent review is more prevalent among small schemes compared to large schemes. Further consideration surrounding the assurance over the controls and procedures for these types of areas will need to take place over the coming year with the expected requirements of the new Code of Practice from the Pensions Regulator due to be issued in October 2022

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



# 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

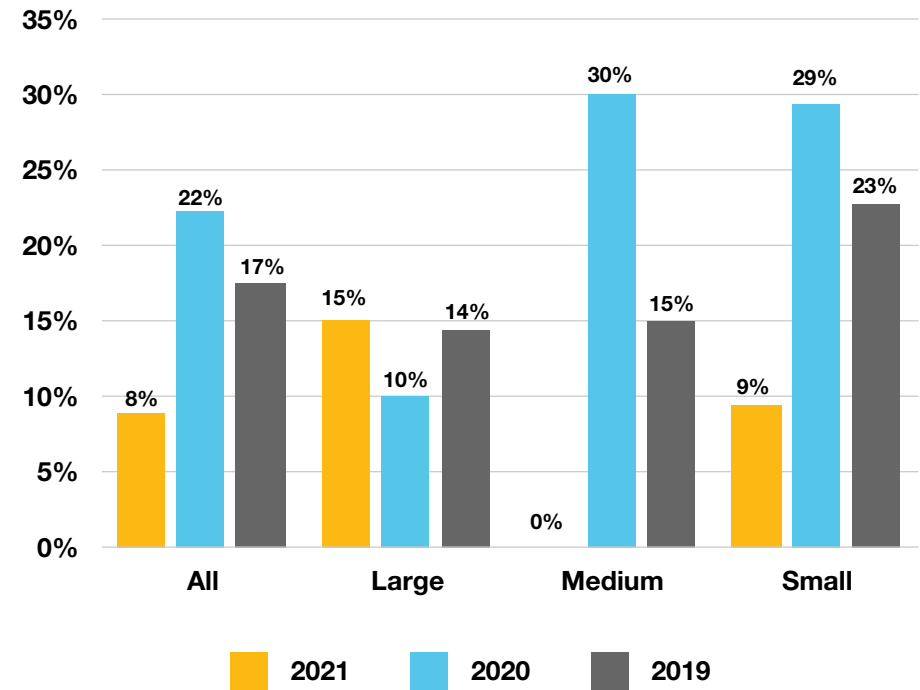
Identified the key operations, IT systems and information flows vulnerable to cybercrime.

2

Assessed the vulnerability of their third party suppliers to cybercrime.

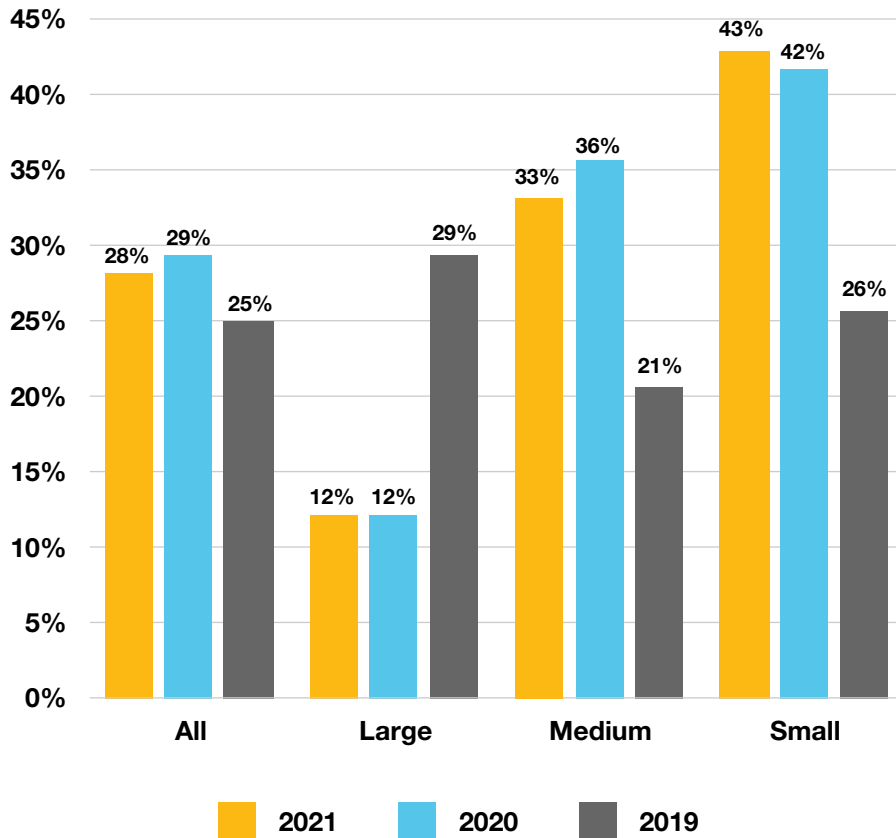
Figures 5 and 6 provide the responses for these two points for years 2021, 2020 and 2019.

Figure 5: Percentage of respondents that have not identified the key operations, IT systems and information flows vulnerable to cybercrime





**Figure 6: Percentage of respondents that have not assessed the vulnerability of their third-party suppliers to cybercrime.**



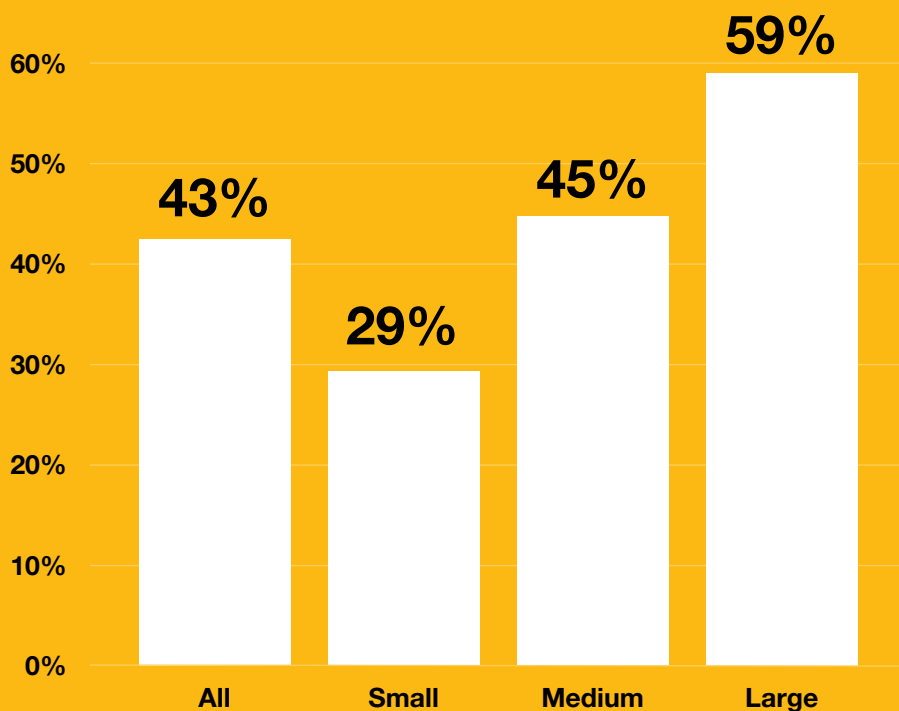
The results show a positive trend in the identification of key operations, IT systems and information flows vulnerable to cybercrime with only 8% of overall respondents confirming that they had not identified these vulnerabilities. However, for larger schemes the trend shows an increase in schemes that are unaware of their cybercrime vulnerabilities and therefore, unlikely to be managing cyber risks effectively.

The majority of pension scheme activities are 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, 28% of all schemes have not assessed the vulnerability of their third-party suppliers to cybercrime. The figures range from 43% for small schemes, 33% for medium schemes, and 12% for large schemes. Over a third of pension schemes have not identified cybercrime vulnerabilities posed by third-party suppliers, and so cannot obtain assurance that the risks are being managed appropriately.

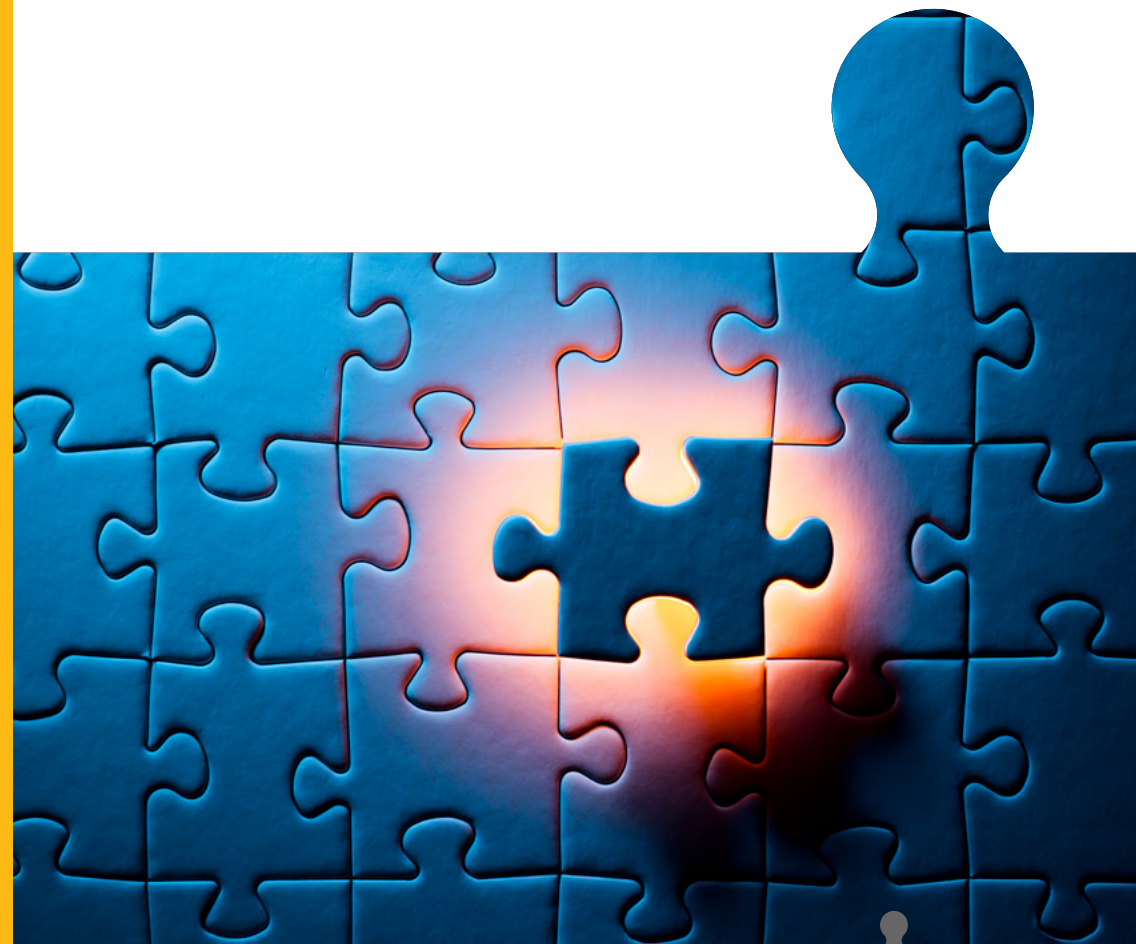
These results are concerning, especially given that cybercrime has been ranked as one of the top risks for DB and DC schemes in the previous two years and is so prevalent at present.

Our survey asked whether Trustees had tested the strength of the Scheme's IT systems, processes and procedures for cybercrime protection.

**Figure 7: Percentage of respondents that have not tested the strength of the scheme's IT systems, processes and procedures for cybercrime protection**



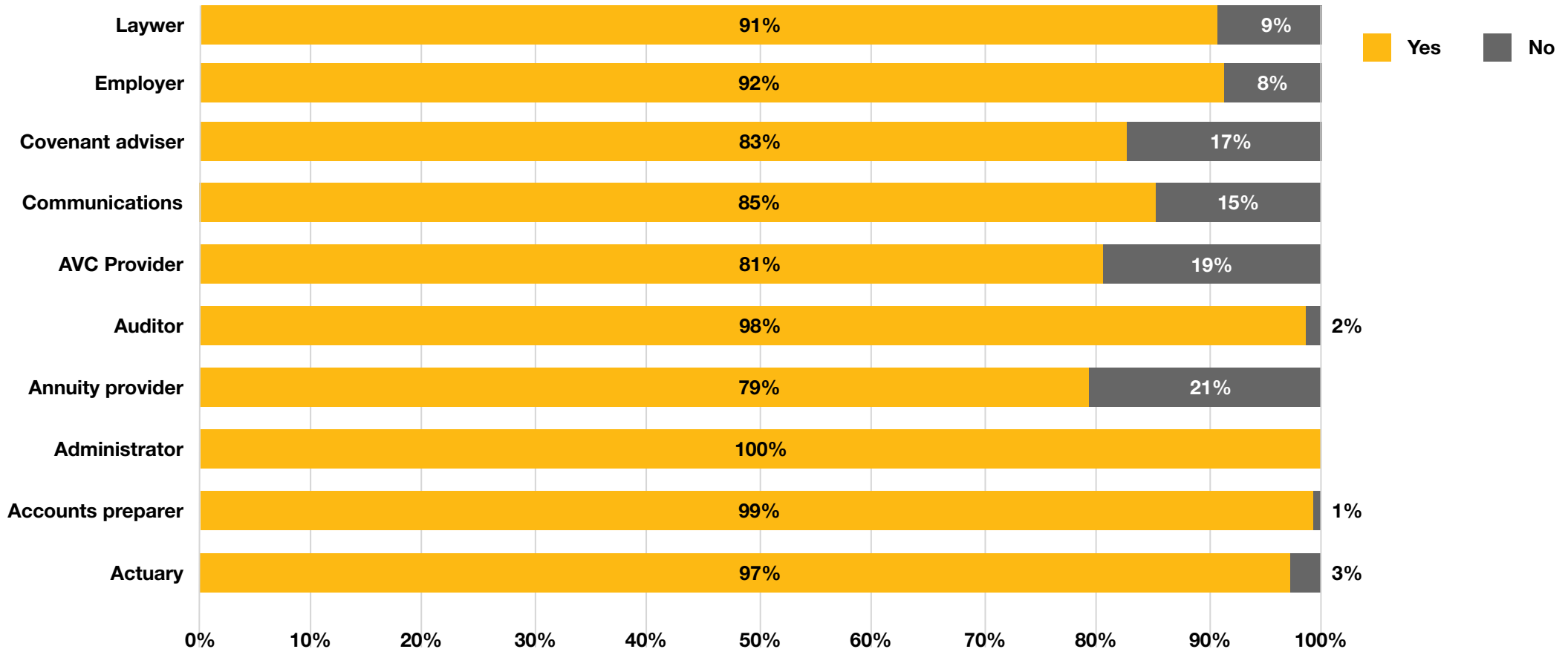
43% of respondents have not tested the cyber resilience of their scheme's IT systems, processes and procedures. The results show that the issue is more prevalent among small and medium schemes compared to large schemes. From our review of the type of schemes that responded, the majority are administered by third-party administrators, therefore we assume that Trustees have not considered it necessary to test the administrators' systems. We recommend that Trustees obtain independent assurance concerning the extent to which their administrators are cyber resilient, in accordance with the National Cyber Security Centre's (NCSC) Cyber Assessment Framework.



# Cybercrime protection – policies

With the introduction of the new Code of Practice later in the year and the increased sophistication of criminals to intercept data, it is fundamental to the protection of scheme data to have a policy in place with the pension scheme's third-party suppliers.

Figure 8: Have you got a policy in place covering the data requirements and how this is transferred securely to the following suppliers?



It is surprising to see that the only supplier where 100% of respondents confirmed that there was a policy in place, was the administrator. For all other suppliers the confirmation that there was no policy in place ranged for 1% (accounts preparer) to 21% (annuity provider). It is imperative that Trustees review the suppliers that data is transferred to and from, and a policy is put in place covering the data requirements with confirmation that this needs to be transferred securely to the supplier.

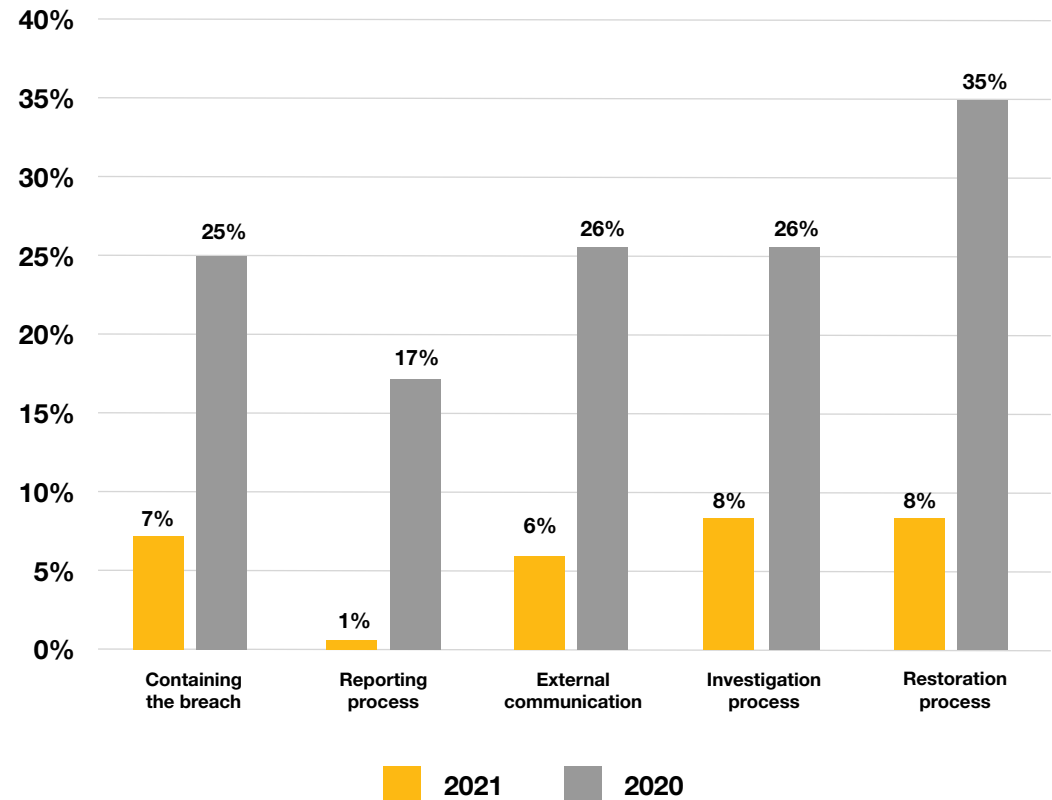


# Cybercrime protection – cyber incident response plan

Fraud and cybercrime are the crimes of the 21st century, accounting for over half of all crime in England and Wales. Cybercrime alone has increased by 113% between April 2020 and the end of September 2021. Despite the prevalence of cybercrime and the potential impact on pension schemes, there are still 5% of schemes which do not have a cyber incident response plan in place (2020: 13%). From experience, Crowe believes this may be an underestimate.

It is encouraging to see the progress that schemes have made over the last year with an increase in the inclusion of the five main areas that we would expect to form part of a cyber incident response plan (figure 9).

Figure 9: Percentage of respondents that do not have the following actions included in their cyber incident response plan.





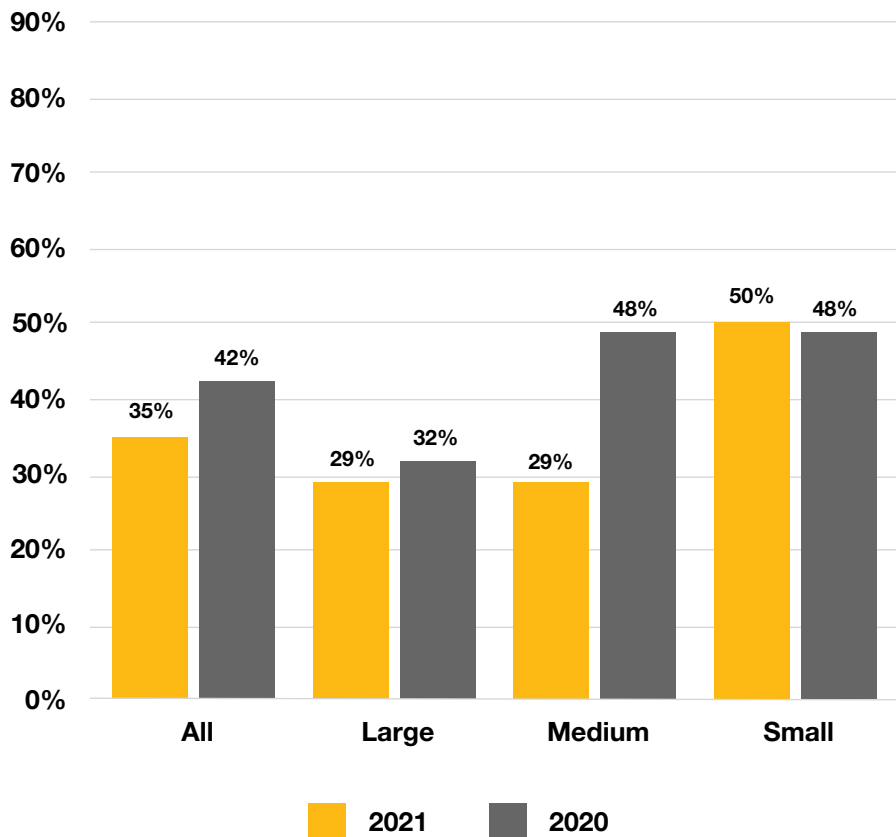
# Cybercrime protection – investigation, training and insurance

We asked respondents whether:

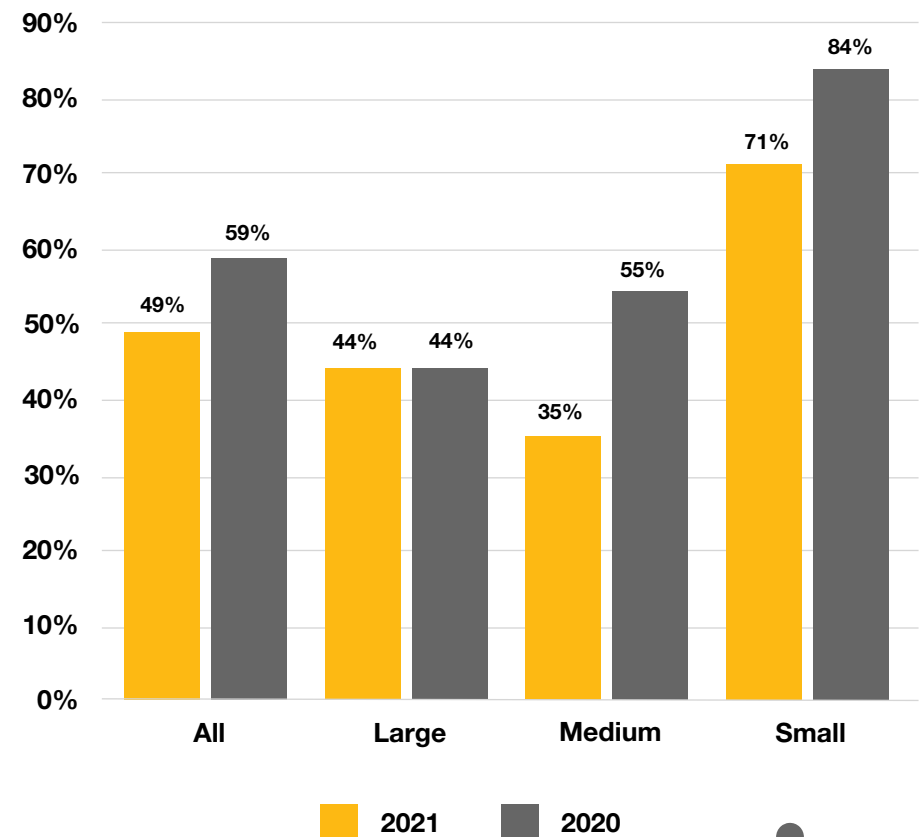
- they have access to the specialist skills needed to help investigate the nature of a cyber breach
- the Trustees received cybercrime scenario-based training.

Despite identifying cybercrime as one of the top risks, 35% of all schemes do not have access to specialist skills and 49% have not provided cybercrime scenario-based training to Trustees (figure 10 and figure 11). 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 10: 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**

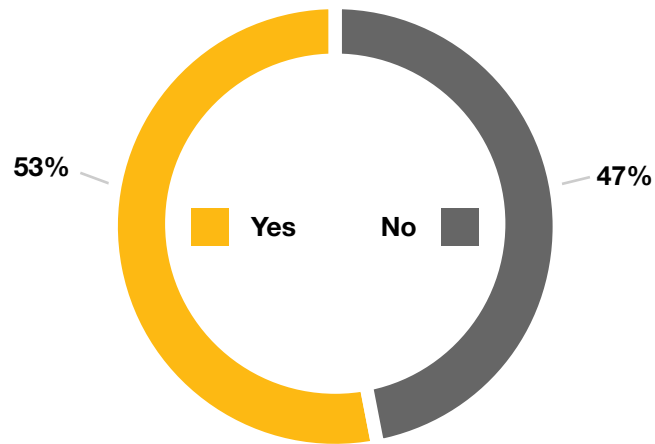


**Figure 11: Percentage of respondents that have not received cybercrime scenario-based training**



# Insurance

Figure 12: Do you have insurance covering the event of a cybercrime attack?

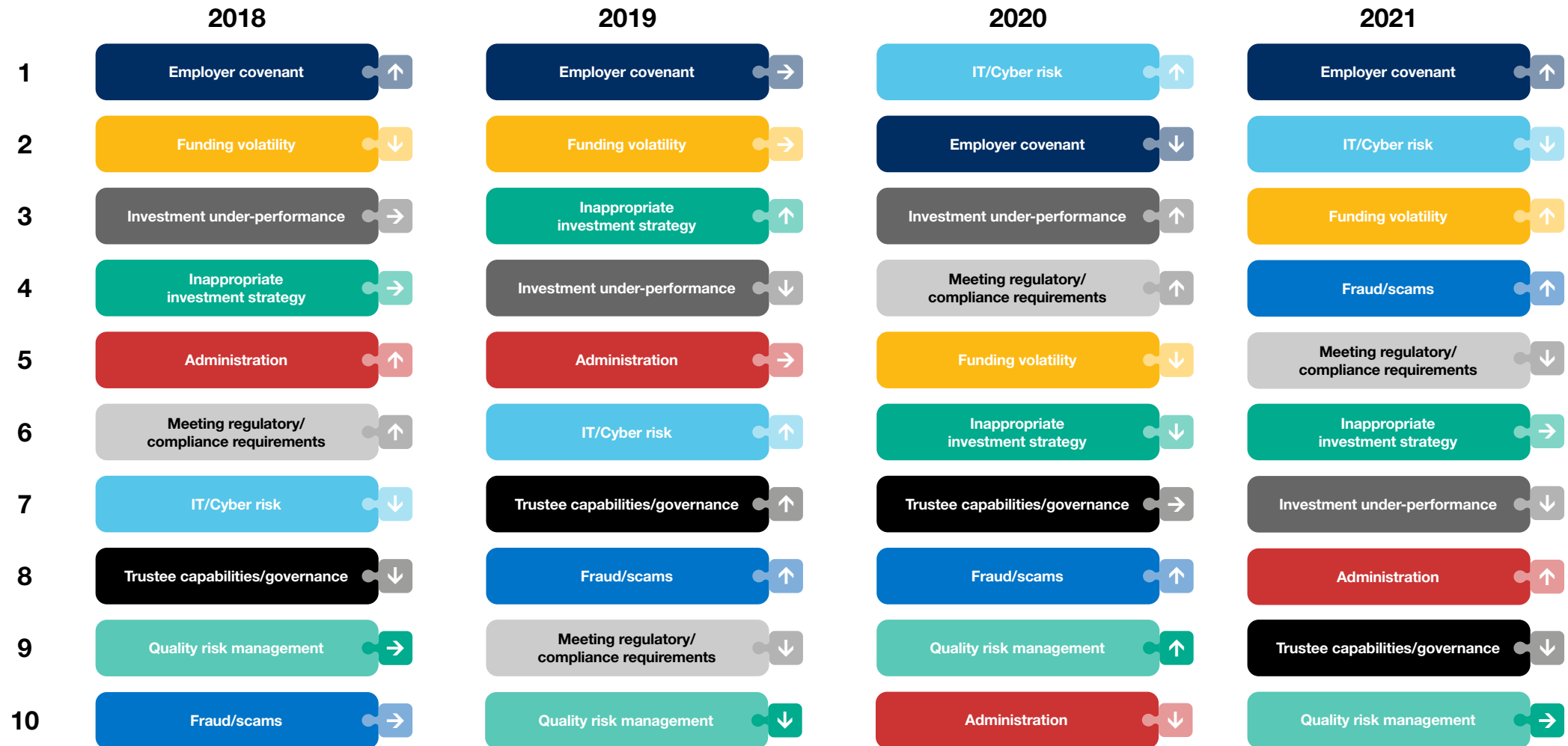


# 53%

Over a half of respondents confirmed that they have insurance covering the event of a cybercrime. Where no insurance is held, Trustees should consider the benefits of taking out suitable insurance



# Defined Benefit (DB) top pension risks trends





In the current year there has been a switch at the top between ‘employer covenant’ risk and ‘IT / Cyber’ risk, with employer covenant taking the top spot in 2021. In turn, ‘funding volatility’ risk has gone to third on the list representing the turbulent world economy over the past year.

The biggest mover was the ‘fraud / scams’ risk, which moved from eighth to fourth in the year. This is not a surprise given the current climate and that pension schemes are not only an attractive target to cyber criminals but also other types of fraud.

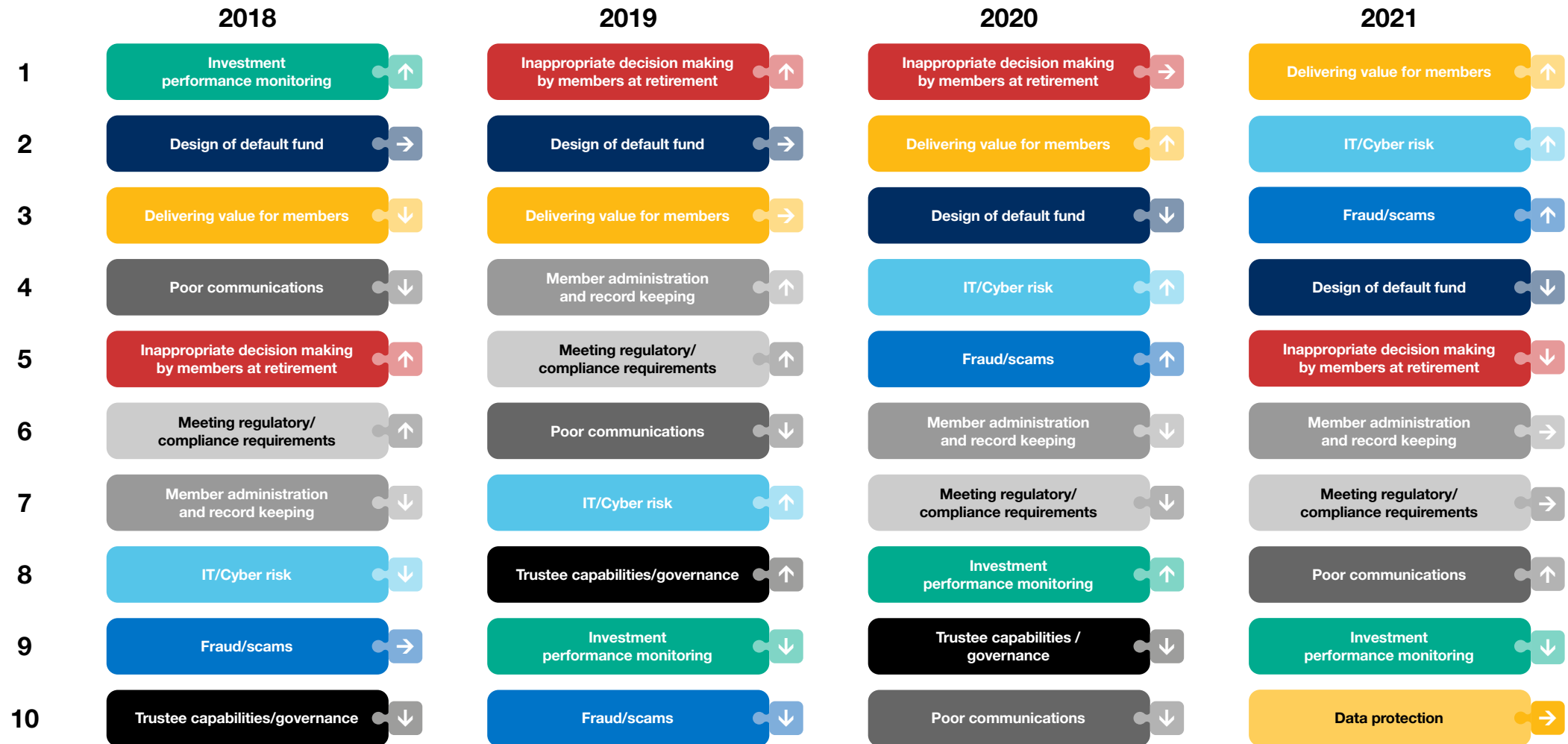
Other notable moves were:

- ‘Administration’ risk which dropped outside the top 10 risks last year has moved to eighth on the list, which may reflect the increased focus on data quality with schemes considering actions they need to take on Guaranteed Minimum Pension (GMP) reconciliations and equalisation.
- ‘Meeting regulatory / compliance requirements’ risk has moved down to fifth this year. It will be interesting to see what happens to this risk following the publication of the Pensions Regulator's new Code of Practice later in 2022.





# Defined Contribution (DC) top pension risks trends



The biggest mover was 'Inappropriate decision making by members at retirement' which has been the top risk for the past two years, now down to fifth on the list. This may be due to Trustees considering that they have put in place appropriate communication to members to enable them to make an informed decision.






'IT / Cyber' risk (second) and 'fraud / scams' risk (third) are high on the agenda for Trustees. This is not a surprise given the attractive nature of pension scheme data and the current climate.

When analysing the risk between the size of the scheme, the only notable difference was that 'delivering value for members' risk and 'design of default fund' risk were the top risk for small schemes, which relates to the resources available for these types of schemes.



# Conclusion

Incidents of cybercrime data issued by ONS 2021 has shown that cybercrime and fraud numbers are increasing and we anticipate that this upward trend will continue. We have summarised five key questions that Trustees should be asking their advisors:

-  What controls and processes does your administrator have in place to counter fraud, especially in the process of changing members' data and how they vet new staff with access to member data?
-  Does your administrator use electronic ID verification for UK and overseas member events and if not, why not?
-  Have you assessed the vulnerabilities of your third-party suppliers to cybercrime?
-  Are you aware of your cybercrime vulnerabilities and how cyber risks are being managed?
-  Do you have policies in place covering the data requirements and how this is transferred securely to all your relevant suppliers?



# 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 impact of cybercrime.

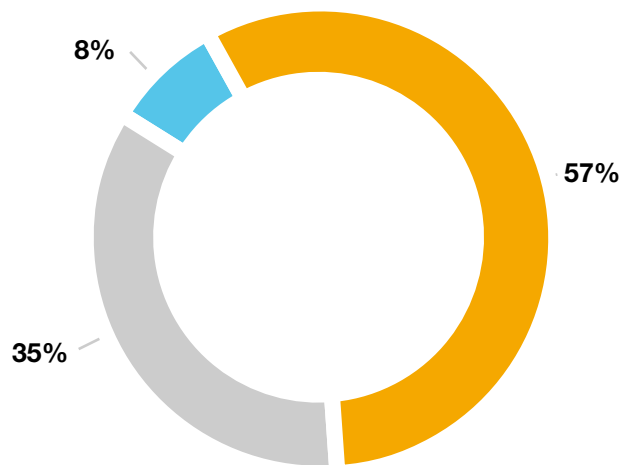




# Appendix: Summary of participants

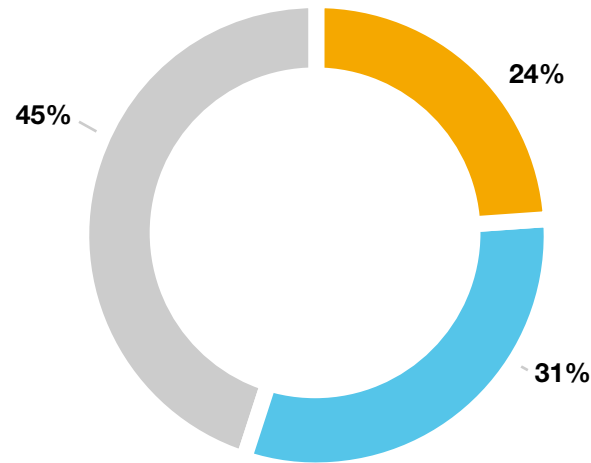
In total, we had 93 responses to our survey, covering a broad range of occupational Trust based pension schemes in the UK. The breakdown by type of pension scheme, size by net assets and members can be found below.

### Type of pension arrangement



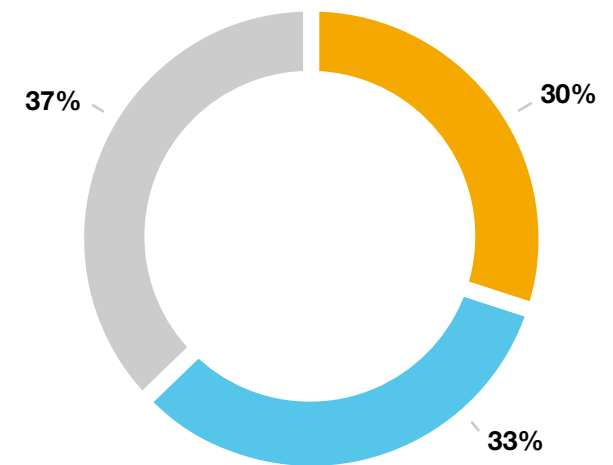
- Trust based DB
- Trust based DC
- Hybrid (i.e. both DB and DC)

### 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

## About Us

Crowe UK is a leading audit, tax, advisory and risk firm with a national presence to complement our international reach. We are an independent member of Crowe Global, one of the top 10 accounting networks 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 businesses of all sizes, professional practices, social purpose and non profit organisations, pension funds and private clients.

We work with our clients to build something valuable, substantial and enduring. Our aim is to become trusted advisors to all the organisations and individuals with whom we work. Close working relationships are at the heart of our effective service delivery.

  @CroweUK |  @Crowe\_UK

[www.crowe.co.uk](http://www.crowe.co.uk)

Crowe U.K. LLP is a member of Crowe Global, a Swiss verein. Each member firm of Crowe Global is a separate and independent legal entity. Crowe U.K. LLP and its affiliates are not responsible or liable for any acts or omissions of Crowe Global or any other member of Crowe Global. This material is for informational purposes only and should not be construed as financial or legal advice. You are encouraged to seek guidance specific to your circumstances from qualified advisors in your jurisdiction. © 2022 Crowe U.K. LLP

