

# Firefighters' Pensions Annual Conference - (AGM and reception)

Tuesday 25 October 2022  
18 Smith Square, London

# Agenda

- Chair's welcome and introduction
- Isio: Local Pension Boards and the 2015 Remedy
- Aon: Cyber security and resilience
- The Pension Regulator's new code of practice
- Drinks reception

# Chair's welcome and introduction

Joanne Livingstone

Chair of the Firefighters' Pensions (England)  
Scheme Advisory Board

# Implementing the McCloud Remedy: Local Pension Boards

Colin Dobbie FFA  
25 October 2022

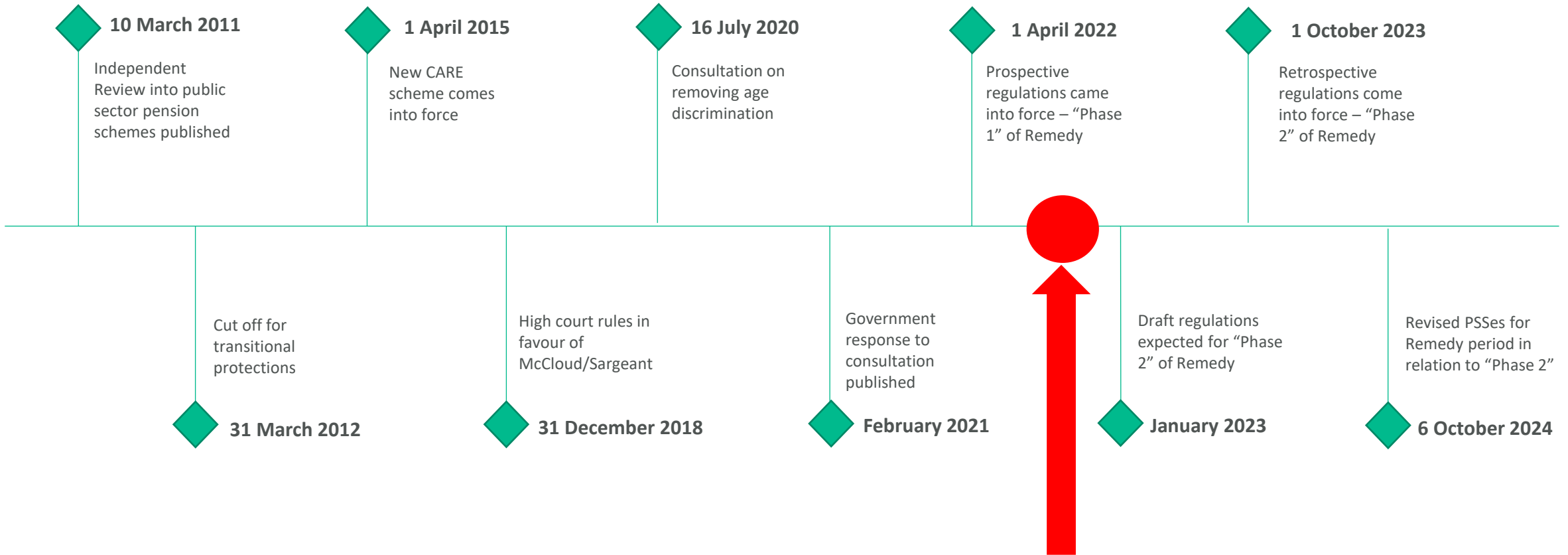
**isio.**



# Agenda

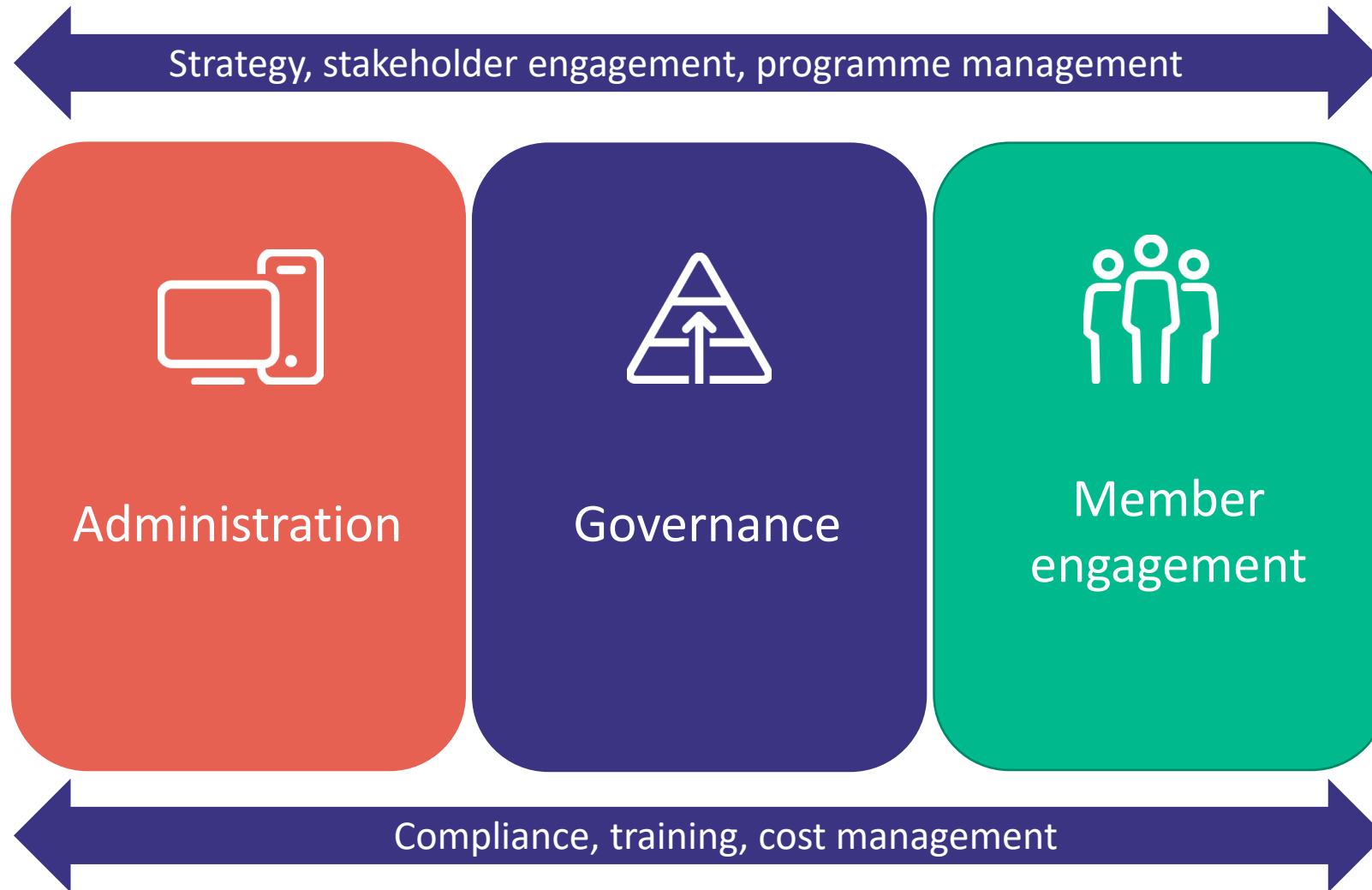
1. Brief history of McCloud Remedy and where are we now?
2. Governance
3. Administration
4. Member engagement
5. Final thoughts

# McCloud timeline



**You are here!**

# 3 pillars of implementing the McCloud Remedy



# Governance

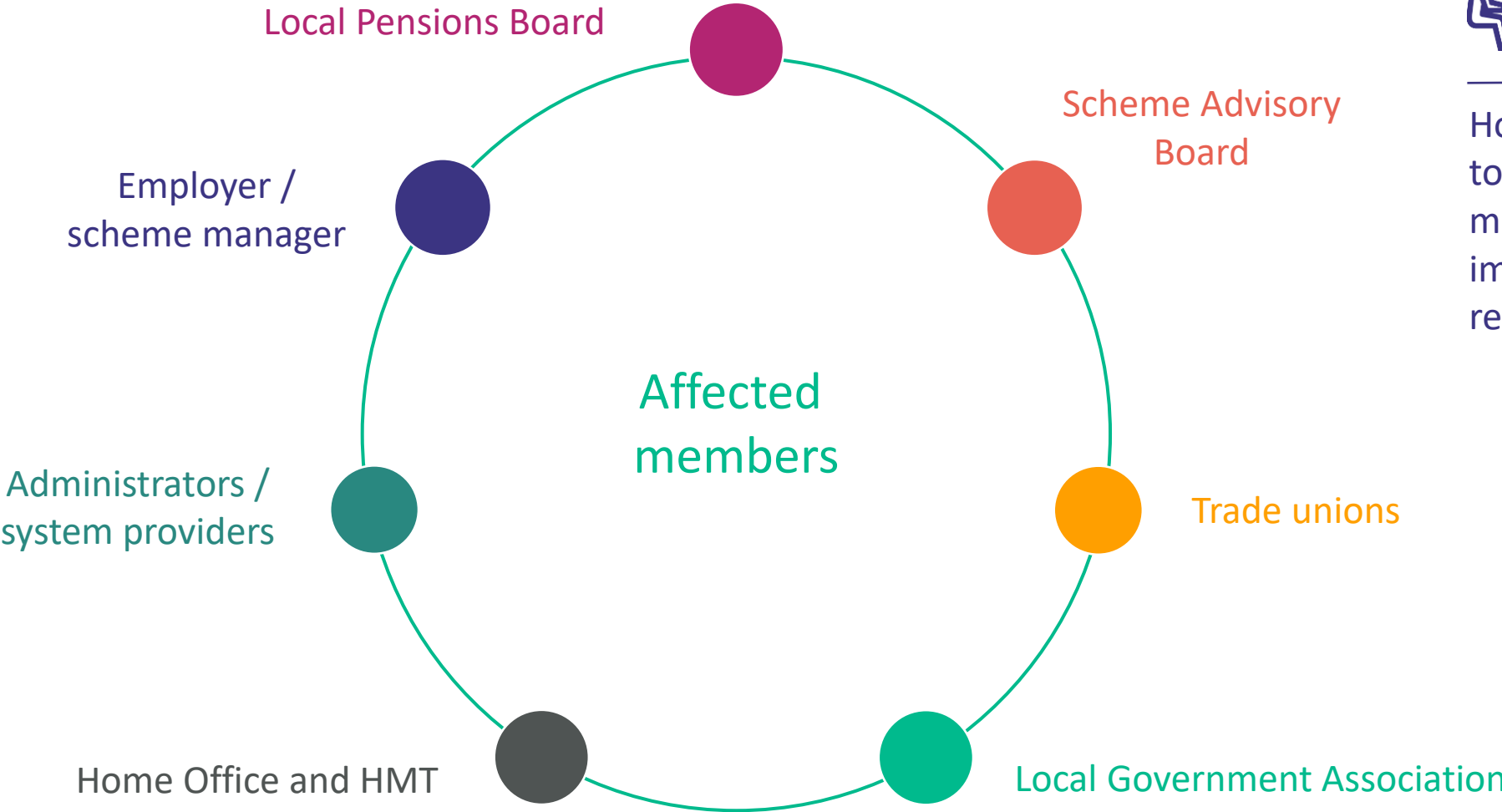


# Governance: Strategy



“The engagement project is an opportunity to re-engage with Scheme members and employers. The approach taken will reflect this, ensuring that every opportunity to modernise and enhance engagement mechanisms and messaging will be taken.” – NHS Pension Scheme

# Governance: Stakeholder engagement



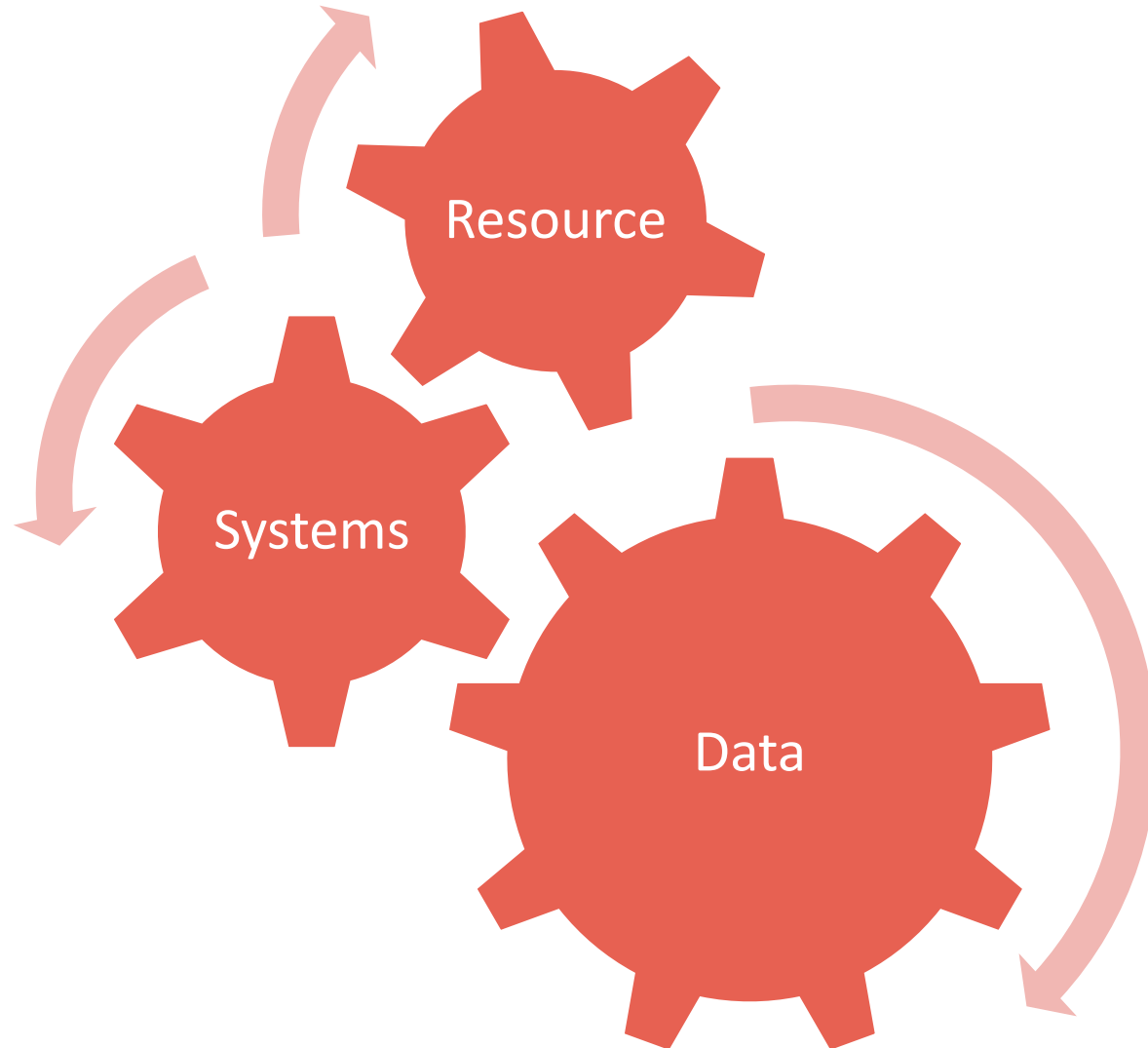
How can stakeholders work together to manage risks and maximise opportunities when implementing the McCloud remedy?

# Governance: Programme management



# Administration

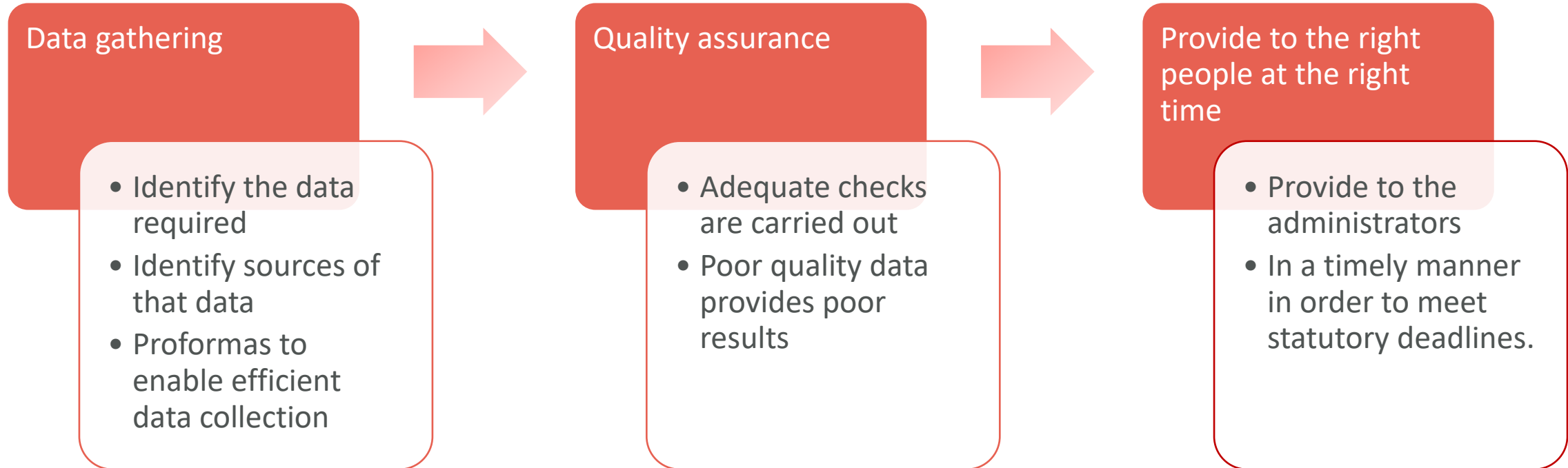
# Administration



---

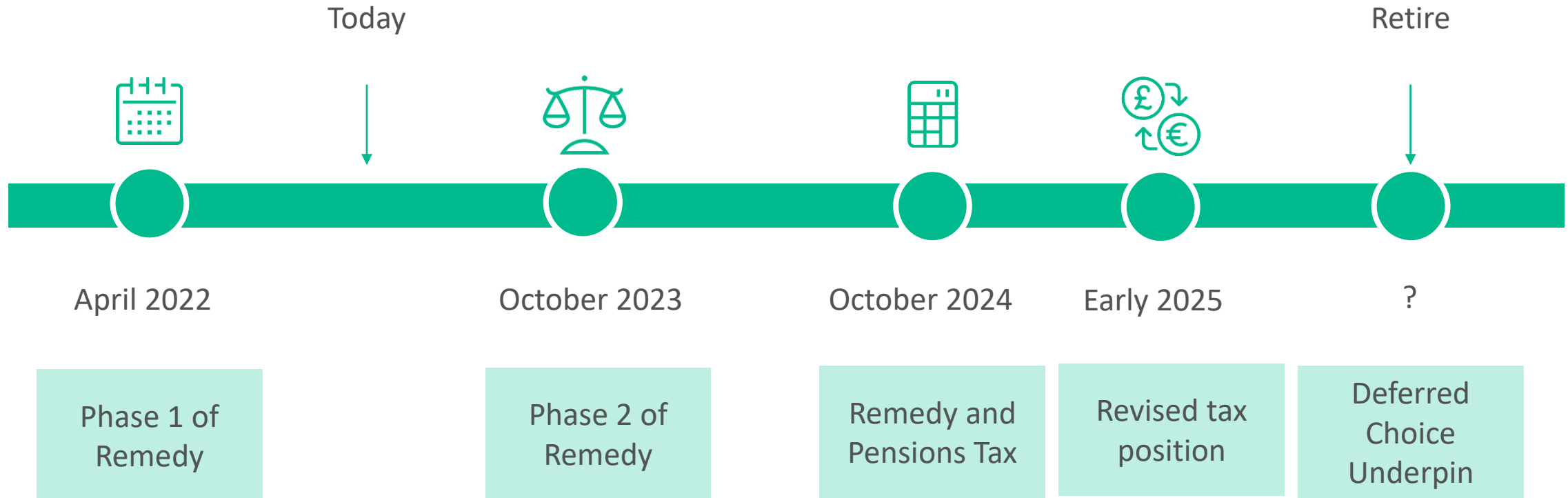
With Scheme managers/Pension Boards pooling together this will present a stronger case for getting the desired updates from systems providers

# Administration: Data



# Member engagement

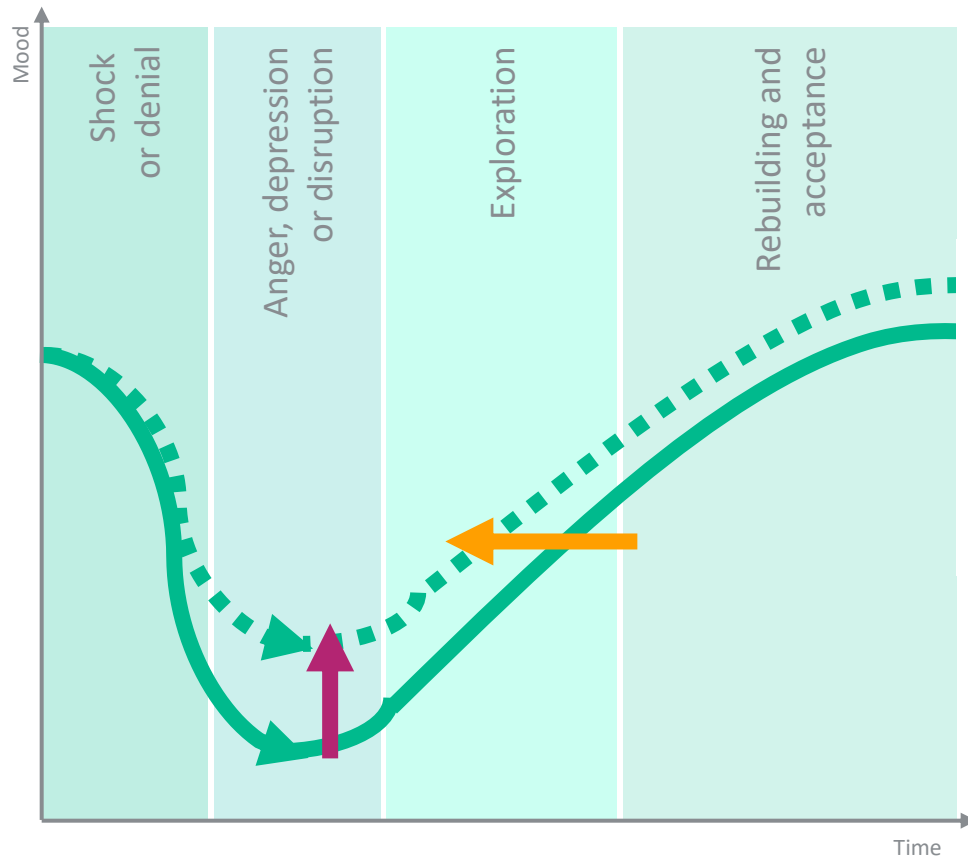
# Firefighter member journey








# Helping member's through a 'change curve'

A typical pensions change project...



Key

-  Reduce negative impact
-  Accelerating change
-  Managed change curve



Engaging with all stakeholders, at the right time and with the right information, is critical

# Where do people go for help?



# Benefits of effective member engagement

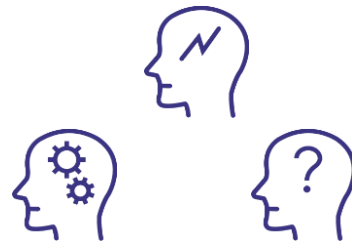
## Build McCloud understanding

---

What? Why? When?

## Manage risk and potential 'noise'

---



## A unique opportunity?

---



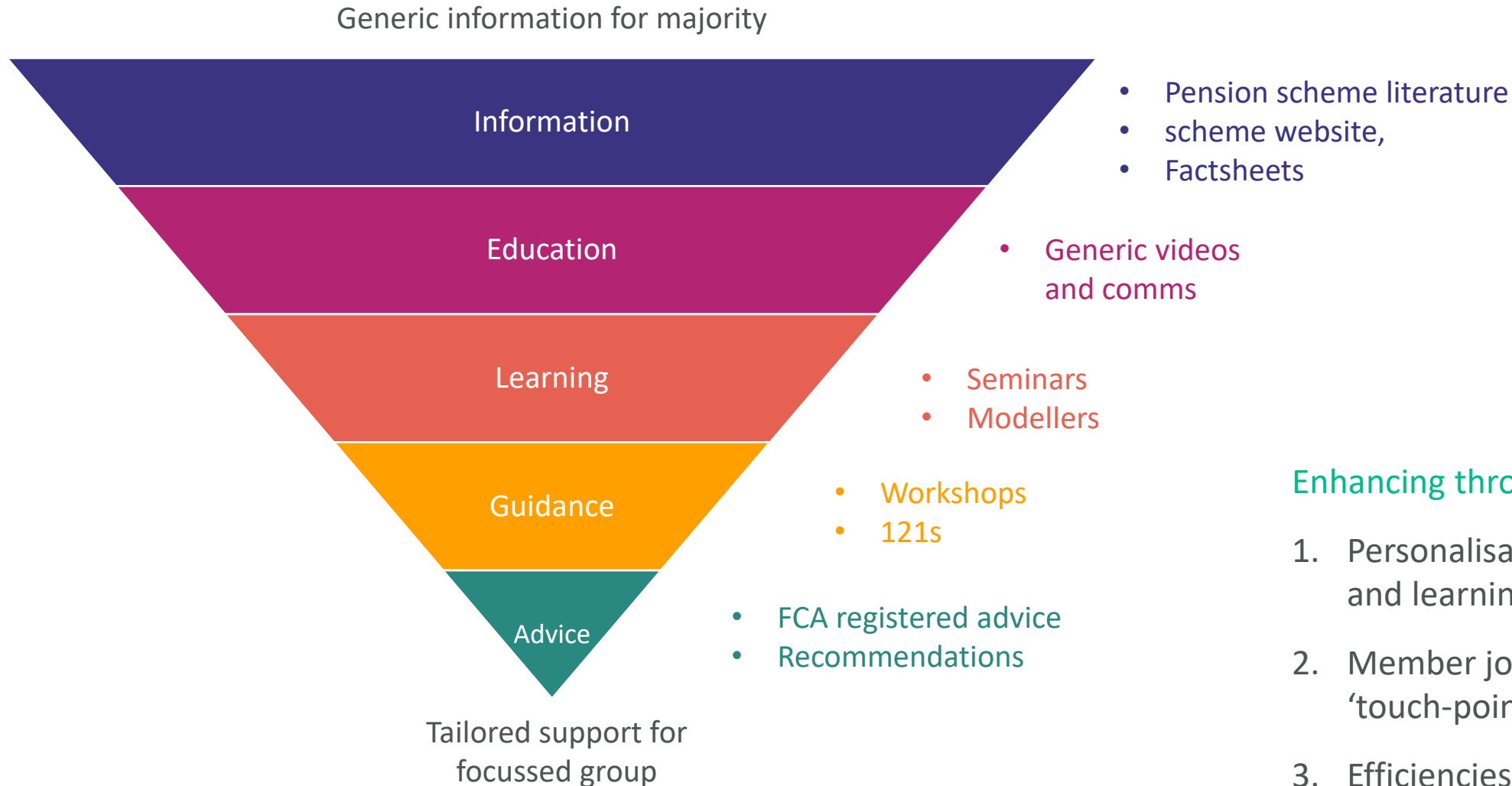
# What does a good engagement strategy look like?

1. Recognises the different groups of members and is designed around to meet their needs
2. Is multi-channel
3. Can be underpinned by technology, but not replace human interaction

---

How do you want your members / employees to feel as they move through their McCloud journey

# Multi-channel communications



## Enhancing through digital

1. Personalisation of information and learning
2. Member journey / intentional 'touch-points'
3. Efficiencies

# Final thoughts

# Final thoughts

1. Continually ask questions, make challenges
2. Opportunity for Scheme managers/Pension Boards to work together
3. Use as a catalyst to re-shape how you approach stakeholder engagement
4. The McCloud Remedy is a positive change for members

---

The McCloud Remedy is a positive change for members, if done right, it can be a positive experience for all

# Thank you

Colin Dobbie

[colin.dobbie@isio.com](mailto:colin.dobbie@isio.com)

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The logo for isio. features the word "isio." in a bold, lowercase, sans-serif font. The letters are white, and the period is a small white dot. The logo is positioned in the bottom left corner of the slide.



# Cyber security and resilience



Presentation to Fire Pensions Annual Conference 2022

Prepared for: FP S AGM

Prepared by: Alison Murray,

Date: 2 Aon 5 October

2022

# Important definitions

## Cyber security

The **protection of devices, services and networks** - and the **information** on them - from **theft or damage** via electronic means

*(from the National Cyber Security Centre)*



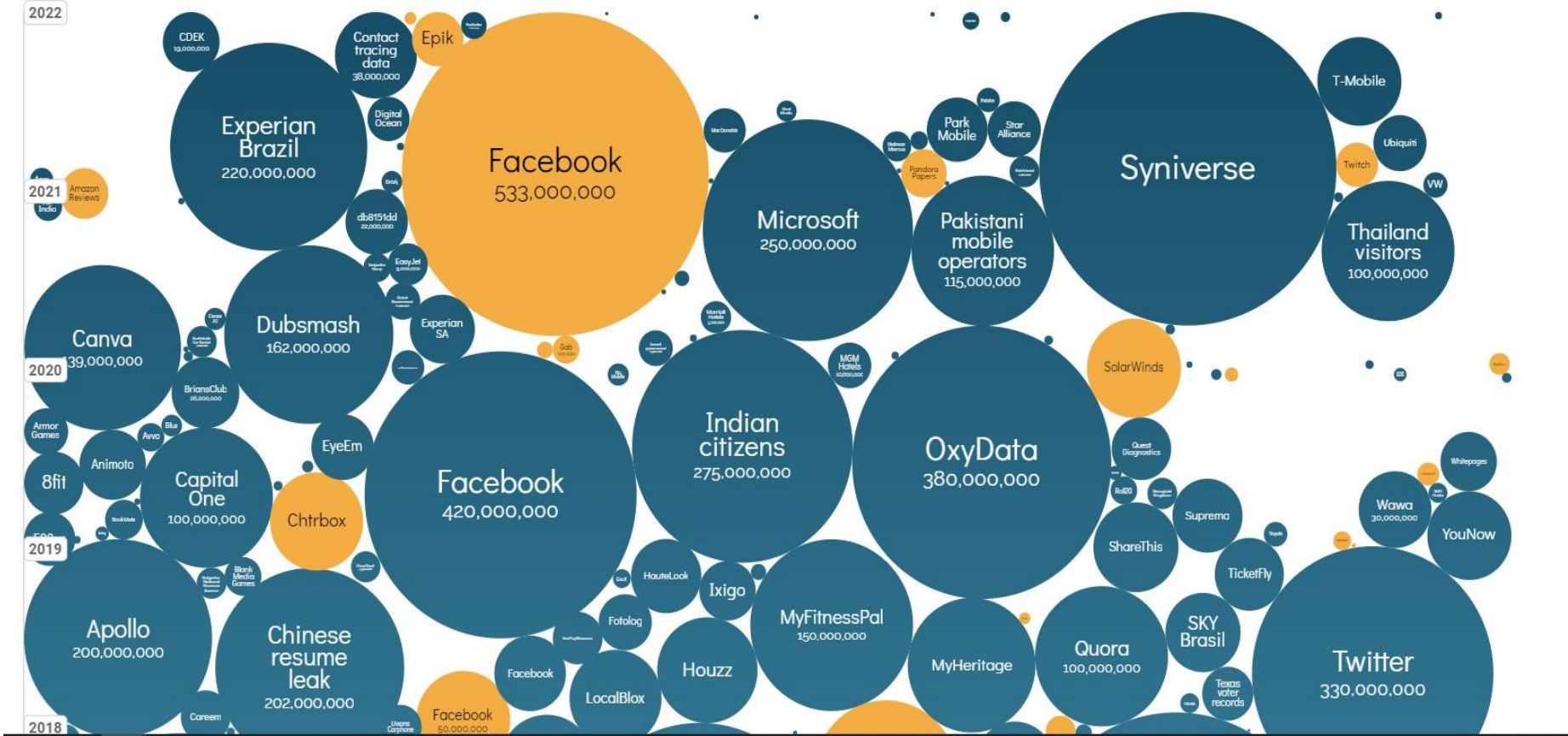
## Cyber risk

The **risk of loss, disruption or damage** to a scheme or its members as a result of the failure of its information technology systems and processes. Includes **risks to information** (data security) as well as **assets**, and both **internal risks** (e.g. from staff) and **external risks** (e.g. hacking).

*(from the Pensions Regulator's Cyber Guidance)*

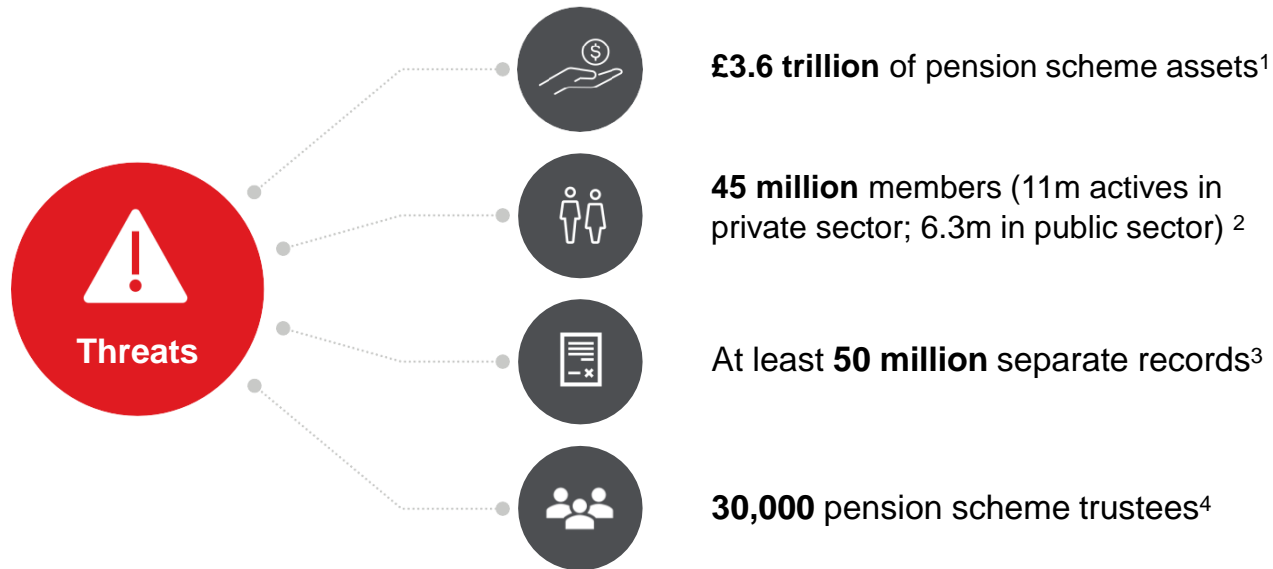
# Cyber threat trends

## World's Biggest Data Breaches & Hacks



Source: <https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

# Are pension schemes at risk?



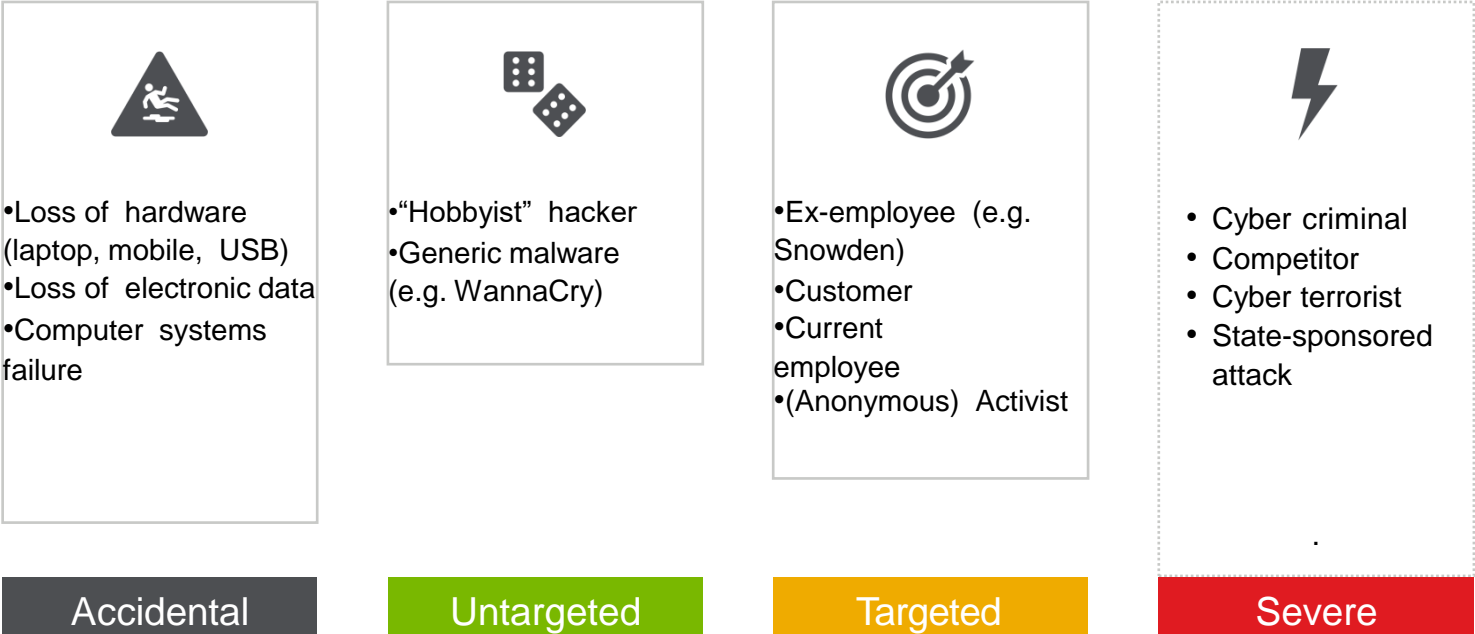
1. Source: OECD Pension Markets in focus 2021 edition

2. Source: Occupational Pension Schemes Survey: UK, 2018

3. Source: Occupational Pension Schemes Survey: UK, 2016

4. Source: Estimated from The Pensions Regulator Trustee Landscape Quantitative Research 2015 and Scheme Return data

# Not all attacks are targeted

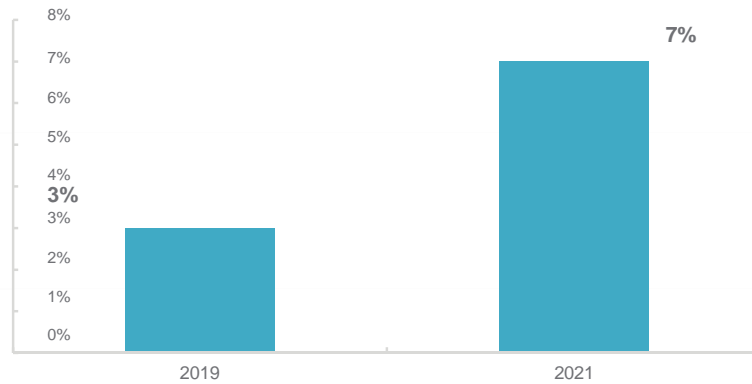


## Key types of attacks

These include - Business Email Compromise, Ransomware and Denial of Service

# Cyber risk is real

Proportion of schemes impacted by cyber incident



Source: Aon Global Pension Risk Survey 2021

## MKCITIZEN

### Cyber attack threat identified in Buckinghamshire and Milton Keynes fire service email

National cyber security watchdogs sent a red alert to Bucks and Milton Keynes Fire Authority after spotting that a "Qakbot" had buried itself in an employee's email.



## NEWS

Home | Coronavirus | Climate | UK | World | Business | Politics | Tech | Science | Health | Family & Education

Technology

### Redcar cyber-attack: Council using pen and paper

### Luton council victim of £1.1m cyber crime

Luton Borough Council was the victim of a 'highly sophisticated and organised crime group' that stole £1.1m that had been earmarked for a local school, investigation reveals.



## The News

### Hampshire's Police Federation comes under cyber attack from hackers

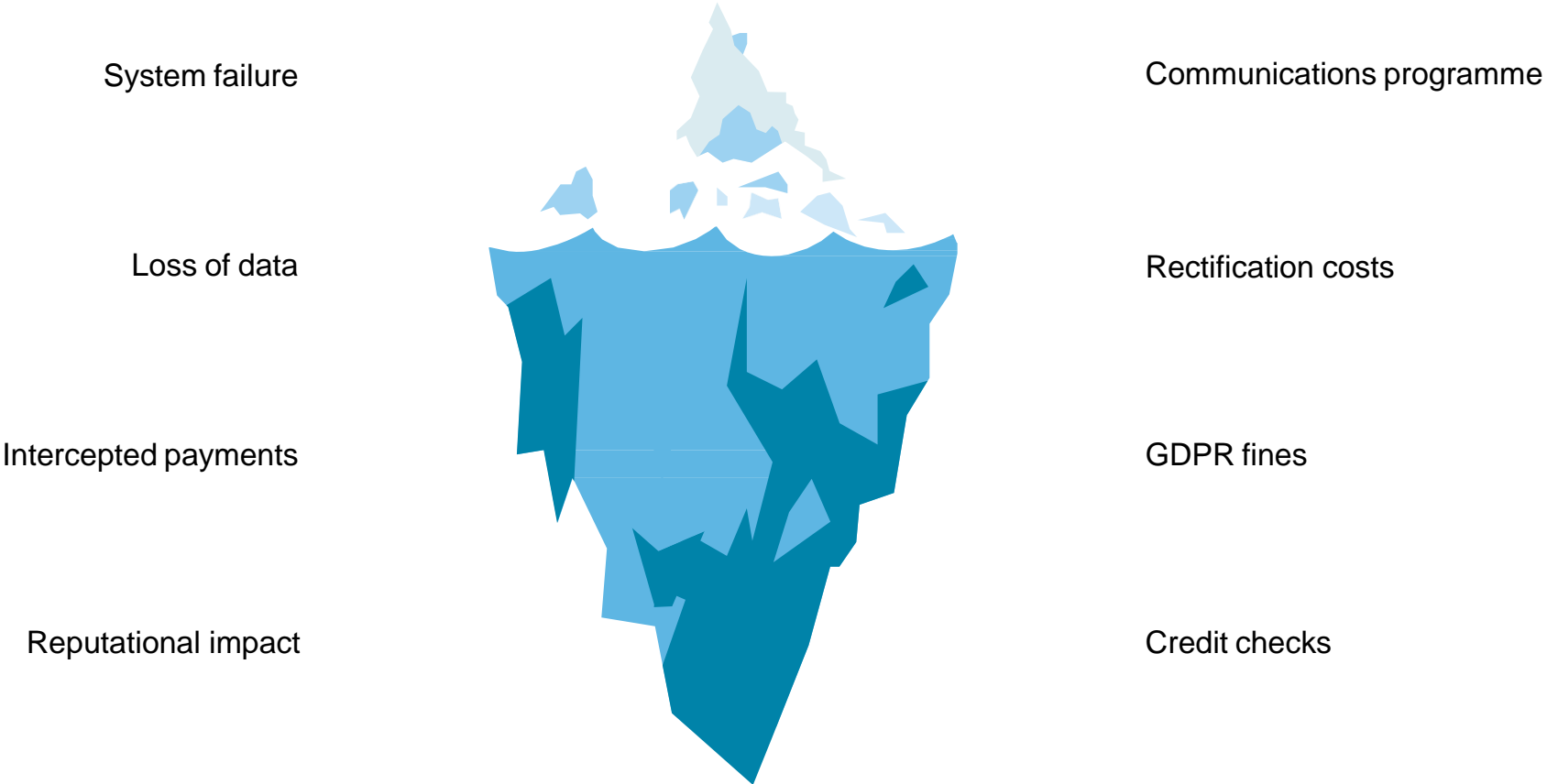
The organisation which represents rank-and-file police officers in Hampshire has been affected by a cyber attack directed at its national body.



## 2020/21 TPR Public Service Pension Scheme Survey

1/3<sup>rd</sup> of public service pension schemes experienced some kind of cyber breach or attack

# Pension scheme consequences



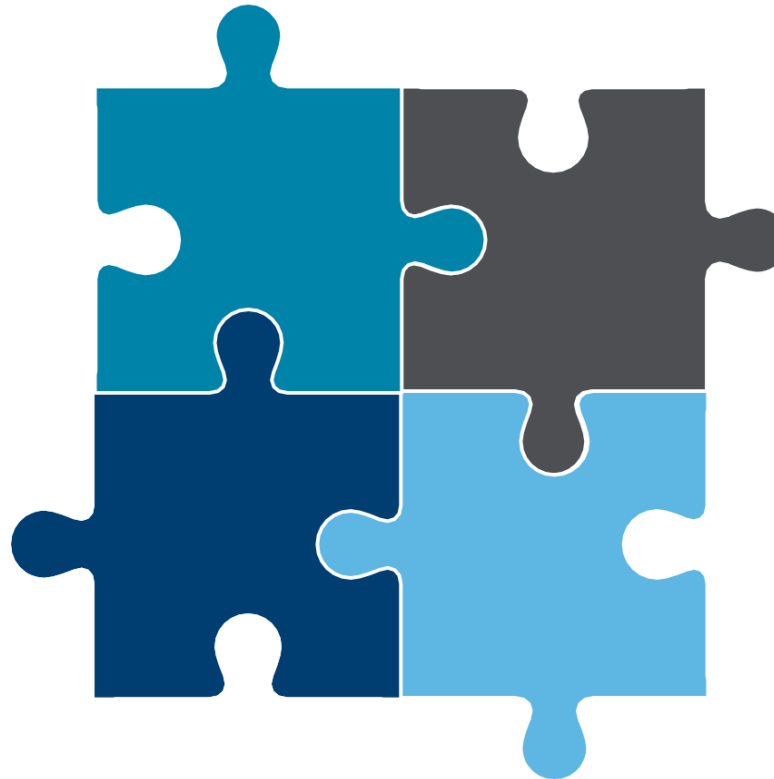
# The Pensions Regulator – 2018 guidance

Roles and responsibilities should be clearly **defined, assigned and understood**

Cyber risk should be on your scheme's **risk register** and regularly reviewed

You should have access to the **required skills and expertise** to understand and manage the cyber risk in your scheme

You should ensure sufficient understanding of cyber risk: your scheme's key functions, systems and assets, its '**cyber footprint**', vulnerabilities and impact



You should ensure **sufficient controls** are in place to minimise the cyber risks

You should assure yourselves that all **third party suppliers** have put sufficient controls in place

There should be an **incident response plan** in place to deal with incidents and enable the scheme to swiftly and safely resume operations

You should be clear on how and when **incidents would be reported** to you and others, including regulators



**Don't forget – legal requirements relating to internal controls**

Managing cyber risk is a key element of risk management and managing internal controls



# Cyber controls in new Single Code of Practice

9

## Key Points

- Fund policies, including
  - Data breach protocols
  - Cyber Incident response plan
- Review service provider controls
- Assess, at appropriate intervals, the vulnerability to a cyber incident

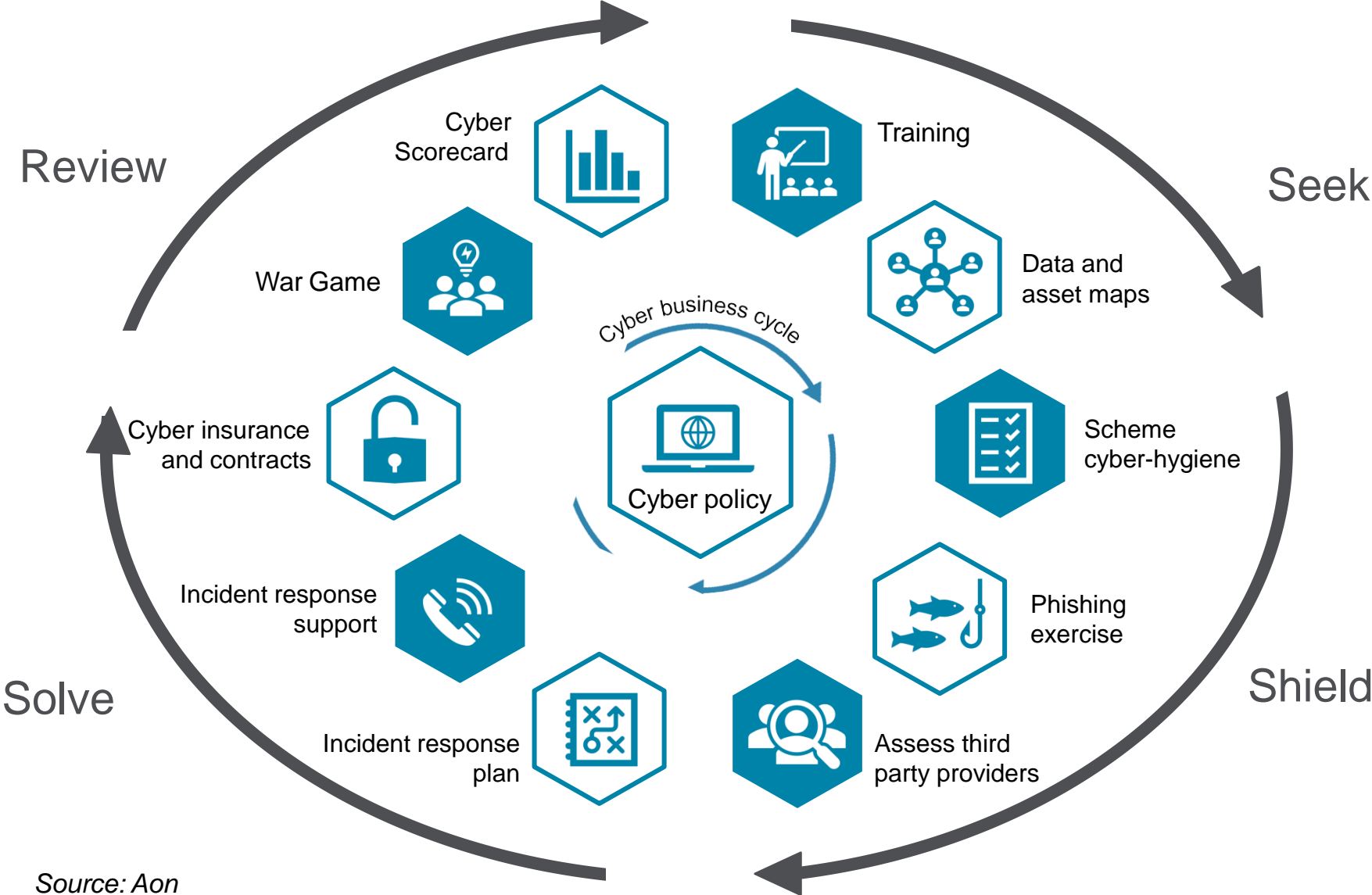


2022 Single Code

## Further information

[New Code of practice \(still draft\): https://www.thepensionsregulator.gov.uk/-/media/thepensionsregulator/files/import/pdf/full-draft-new-code-of-practice.ashx](https://www.thepensionsregulator.gov.uk/-/media/thepensionsregulator/files/import/pdf/full-draft-new-code-of-practice.ashx)

# How might you approach cyber risk management?



Source: Aon

# Seek - understand your interactions

## Host Authority

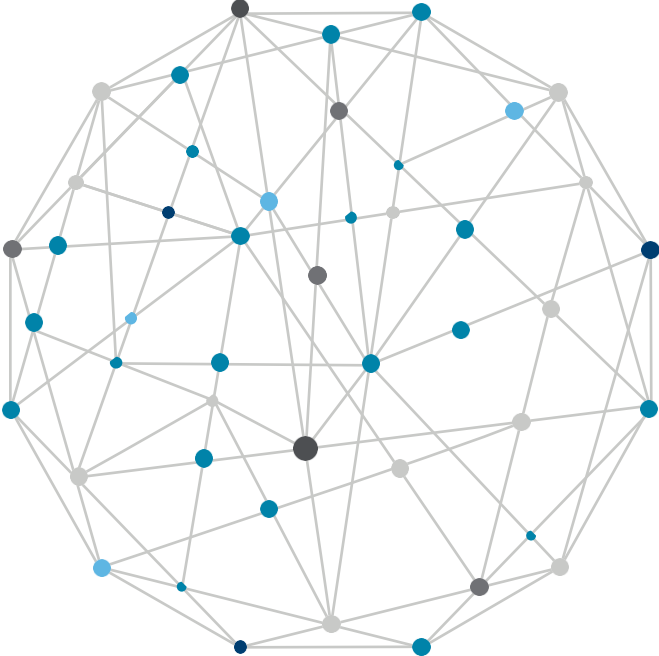
The key provider, supports all you do but you are reliant on them.

## Admin software provider

Given the amount of membership data held, your provider is one of the first lines of defence.

## Internal parties

Local Pension Board, internal audit, sub-committees etc.



## National organisations

NI Database, GAD, HMRC, Tell Us Once, Etc.

## External Advisors

Your Actuary, external auditors and also member advisors like IFAs and legal representatives.

## Other external providers

AVC providers, other pension schemes, IDRPs providers etc.



## Key takeaway

There are a lot of connections when considering data transfer  
Need to build a similar picture to identify touch points/providers for assets/cashflows

# Shield - cyber-hygiene

## Passwords

Do not repeat passwords on different sites

Use long passwords – preferably passphrases.

Include numbers, letters and symbols in your passwords

## Multifactor authentication

Switch on multifactor authentication, wherever available.

## Device security

Keep antivirus software and apps up to date.

Use public Wi-Fi with caution

Look for the lock icon in the URL bar when using the internet.



## Suggestion

Consider developing pension-specific cyber hygiene guidelines in collaboration with the Authority



## Be alert to scams

Phishing still the most popular method

Report suspicious emails.

## Review social media footprint

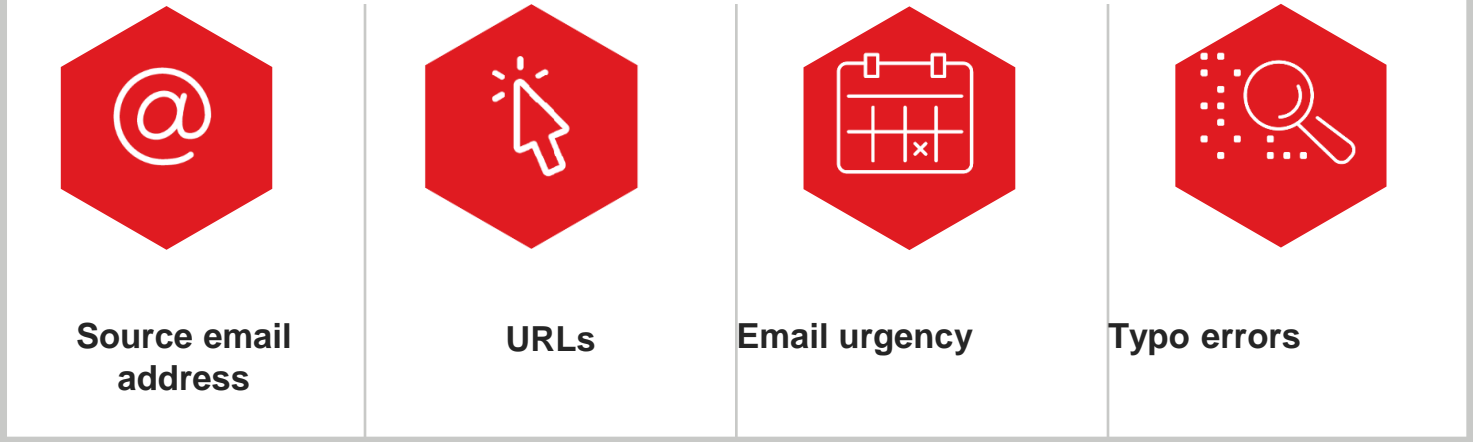
Review what information you and those connected to you post online and consider what information this could divulge.

Report suspicious messages, links and activity

# Features of a phishing email

## Every Phishing email is different

However, there are usually some key features of a Phishing email which might have alerted to the authenticity of the email:

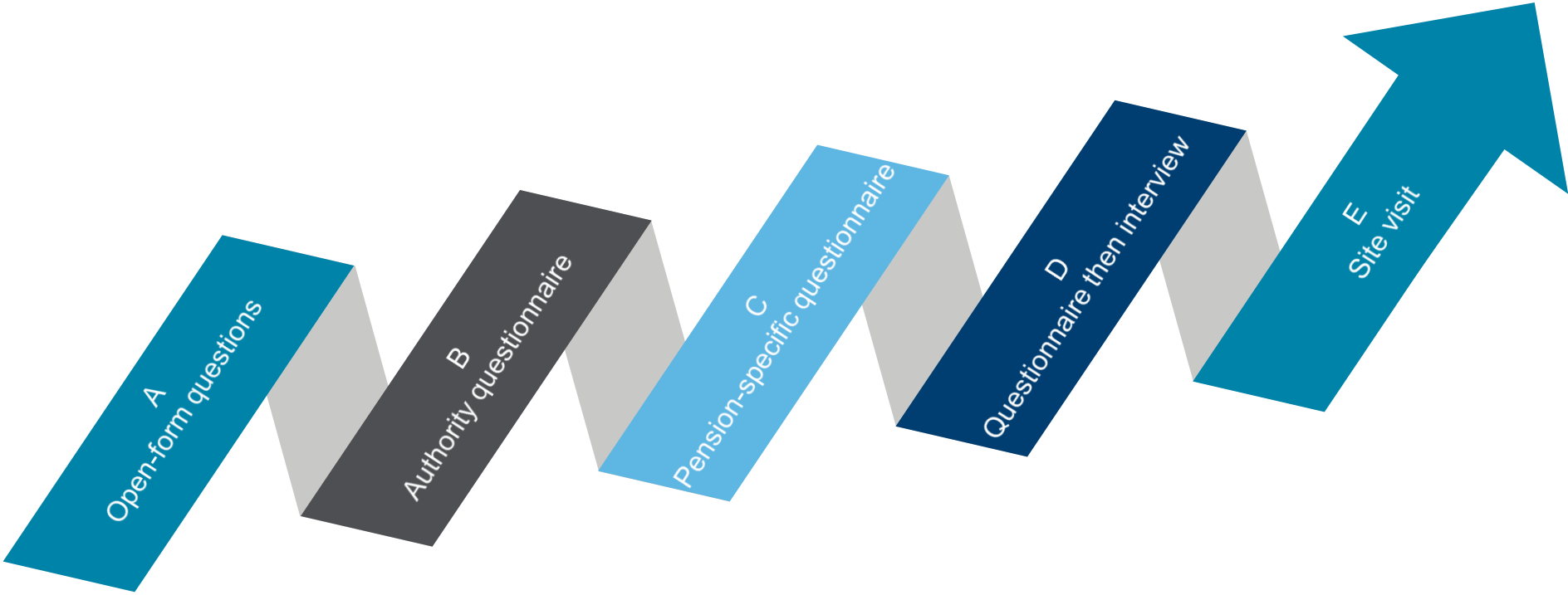


### Action



- Report suspicious emails in line with your internal policy
- For suspicious emails to a personal email address report to NCSC Suspicious Email Reporting Service ([report@phishing.gov.uk](mailto:report@phishing.gov.uk))
- If (personally) you think you might have been a victim of cyber crime visit Action fraud ([actionfraud.police.uk](http://actionfraud.police.uk)) or call 0300 123 2040

# Shield - How to assess third party providers



### Open-form questionnaire

Simplest approach. Each party asked how they deal with cyber risk.

### Authority questionnaire

Relatively common where host authority is large with good existing cyber awareness

### Pension-specific questionnaire

Tend to be better tailored to Fund risks

### Questionnaire then interview

Cyber expert interviews day-to-day contact plus IT supplier to probe on questionnaire responses

### Site Visit

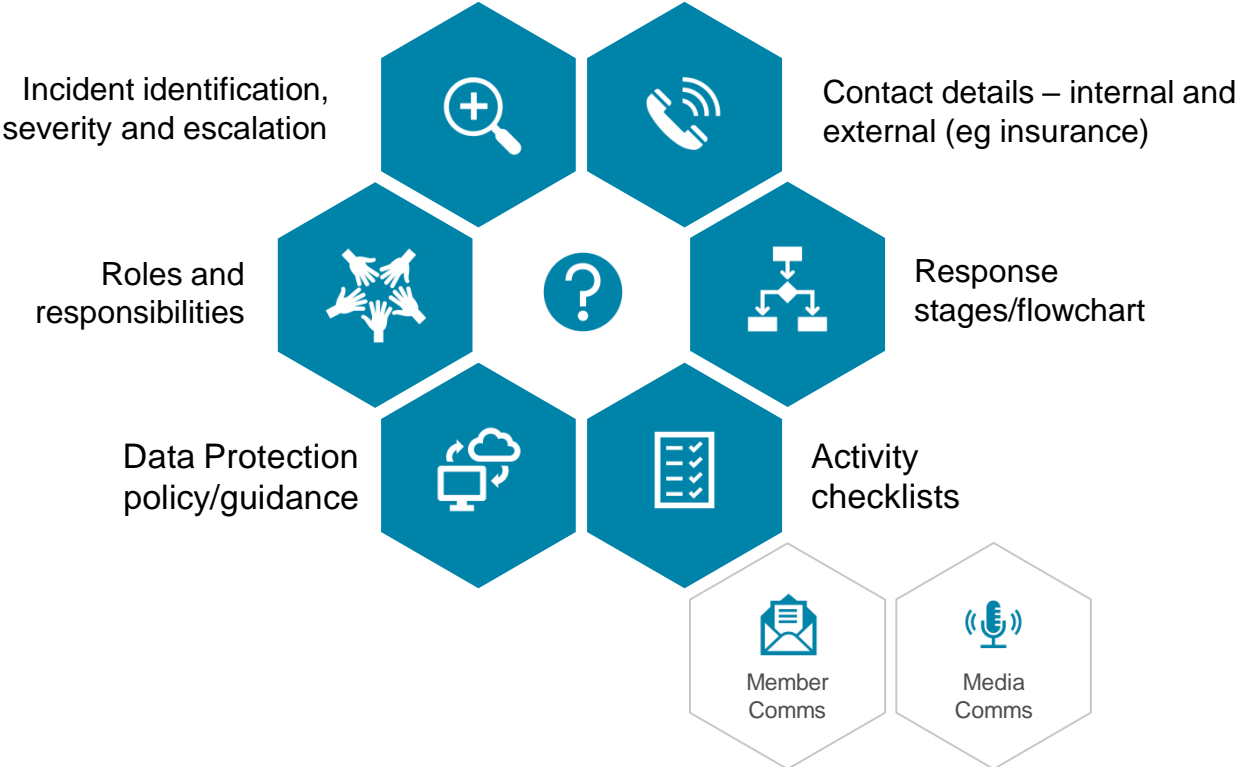
Extension of D to include a full site visit



### Decision

Frequency of reviews and level of detail is required; won't be the same for every provider

# Solve - Incident Response Plan



## Opportunity

Work with your organisation – do they already have an incident response plan? Does it cover pensions?

# Summary

## Cyber is a significant risk

Post pandemic this risk is getting higher, so needs to be high on risk register

## TPR is taking more notice

New code will place more focus on what funds need to do

## Cyber Security Policy

Should include some or all of the ideas covered today

## Needs to be built into BAU

Start with where you are and build resilience from there





# Questions



# Disclaimer

To protect the confidential and proprietary information included in this material, it may not be disclosed or provided to any third parties without the prior written consent of Aon Solutions UK Limited. This presentation may be shared with attendees of the Fire Pension Schemes AGM subject to the conditions listed below. However, this document does not constitute advice to any attendee of the conference, nor does Aon accept any duty of care to any party in relation to this document.

The conditions are as follows:

- Attendees acknowledge and agree that Aon Solutions UK Limited is not providing advice to them and that Aon Solutions UK Ltd does not have any responsibility towards any attendees relying on this material.

Attendees agree that they will not distribute or otherwise communicate any part of the information to any other party without prior written consent of Aon Solutions UK Ltd

In addition, nothing in this document should be treated as an authoritative statement of the law on any particular aspect or in any specific case. It should not be taken as financial advice and action should not be taken as a result of this document alone. Individuals are recommended to seek independent financial advice in respect of their own personal circumstance.

Aon plc (NYSE:AON) exists to shape decisions for the better - to protect and enrich the lives of people around the world. Our colleagues provide our clients in over 120 countries with advice and solutions that give them the clarity and confidence to make better decisions to protect and grow their business.

---

Copyright © 2022 Aon Solutions UK Limited and Aon Investments Limited. All rights reserved. aon.com. Aon Wealth Solutions' business in the UK is provided by Aon Solutions UK Limited - registration number 4396810, or Aon Investments Limited – registration number 5913159, both of which are registered in England and Wales have their registered office at The Aon Centre, The Leadenhall Building, 122 Leadenhall Street, London EC3V 4AN. Tel: 020 7623 55000. Aon Investments Limited is authorised and regulated by the Financial Conduct Authority. This document and any enclosures or attachments are prepared on the understanding that they are solely for the benefit of the addressee(s). Unless we provide express prior written consent no part of this document should be reproduced, distributed or communicated to anyone else and, in providing this document, we do not accept or assume any responsibility for any other purpose or to anyone other than the addressee(s) of this document. In this context, "we" includes any Aon Scheme Actuary appointed by you. To protect the confidential and proprietary information included in this document, it may not be disclosed or provided to any third parties without Aon's prior written consent.





**The  
Pensions  
Regulator**

Making workplace pensions work

# TPR's new code of practice

**FRA AGM**

**25 October 2022**

# The purpose of codes of practice

- Our COPs are not statements of the law, except in certain circumstances set out in legislation. Instead, our COPs set out our expectations for the conduct and practice of those who must meet the requirements set in pensions legislation.
- In most cases there is no specific penalty for failing to follow a COP, or to meet the expectations set out in it.
- However, we may rely on COPs in legal proceedings as evidence that a requirement has not been met. In those situations, a court must take a COP into account when considering their verdict.
- Similarly, if we find grounds to issue an improvement or a compliance notice, they may be worded in relation to a COP issued by us.

# Our codes of practice

Code of Practice	Code in force
01: Reporting breaches of the law	April 2005
02: Notifiable events	April 2005
03: Funding defined benefits	July 2014 (GB), July 2015 (NI)
04: Early leavers	May 2006
05: Reporting of late payment of contributions to occupational pension schemes	September 2013
06: Reporting of late payment of contributions to personal pension schemes	September 2013
07: Trustee knowledge and understanding (TKU)	November 2009
08: Member nominated trustees/member nominated directors – putting arrangements in place	November 2006
09: Internal controls	November 2006
10: Modification of subsisting rights	January 2007
11: Dispute resolution – reasonable periods	July 2008
12: Circumstances in relation to the material detriment test	June 2009
13: Governance and administration of the occupational trust-based schemes providing money purchase benefits	July 2016
14: Governance and administration of public service pension schemes	April 2015
15: Authorisation and supervision of master trusts	October 2018

These slides remain the property of The Pensions Regulator and their content should not be altered on reproduction.

# The catalyst for change

- The OPS (Governance) (Amendment) Regulations (2018)
- Required us to draft new expectations for “effective systems of governance” and “own risk assessment”
- On review of the current codes we found many issues of outdated, duplicate and inconsistent expectations

# Issues with codes of practice

Code of Practice	Code in force
01: Reporting breaches of the law	April 2005
02: Notifiable events	April 2005
03: Funding defined benefits	July 2014 (GB), July 2015 (NI)
04: Early leavers	May 2006
05: Reporting of late payment of contributions to occupational pension schemes	September 2013
06: Reporting of late payment of contributions to personal pension schemes	September 2013
07: Trustee knowledge and understanding (TKU)	November 2009
08: Member nominated trustees/member nominated directors – putting arrangements in place	November 2006
09: Internal controls	November 2006
10: Modification of subsisting rights	January 2007
11: Dispute resolution – reasonable periods	July 2008
12: Circumstances in relation to the material detriment test	June 2009
13: Governance and administration of the occupational trust-based schemes providing money purchase benefits	July 2016
14: Governance and administration of public service pension schemes	April 2015
15: Authorisation and supervision of master trusts	October 2018

Affected by changes to legislation in April 2015

Outdated approach

Affected by change to legislation in January 2019

# Structure

- Aims for consistency in expectations for all scheme types
- Just over a third the length of the codes it replaces
- Separates content into 5 key areas:
  - The Governing Body
  - Funding and investment
  - Administration
  - Communication and disclosure
  - Reporting to TPR
- Other codes being designed to fit into the new format and framework



# New approaches

- Application
  - DB, DC, PS
  - Master Trusts & CDC
- Guidance uplifted
  - Cyber Security
  - Environmental, social and governance (ESG)
- Broadened expectations
  - Financial transactions

# Web-based code of practice

- The new code is designed to be a web-based product
- Designed for ease of use, simple navigation and an efficient search
- Online look and feel developed alongside code text

Published: 17 March 2021

Scheme managers of public service pensions schemes must publish certain information about the pension board and keep that information up-to-date.

This will ensure that scheme members can easily access information about who the pension board members are, the representation of scheme members on the pension board, and the responsibilities of the board.

Governing bodies may also consider publishing information about pension board business, for example board papers, agendas and minutes of meetings. These may be redacted to the extent that they contain confidential information and / or data protected by data protection legislation. Governing bodies should consider requests for publication of additional information, to encourage scheme member engagement and promote a culture of transparency.

Governing bodies may consider how best to publish information, making use of the principles outlined in [General principles for member communications](#).

The scheme manager must publish and maintain:

- the names of pension board members
- details about the representation of scheme members on the pension board
- details of the matters for which the pension board is responsible<sup>R(1)</sup>

Governing bodies may also publish:

- the employment and job title (where relevant) and any other relevant position each board member holds
- details of the pension board recruitment process
- who each pension board member represents
- the full terms of reference for the pension board, including details of how it will operate
- any specific roles and responsibilities of individual pension board members

Governing bodies should:

- have policies and processes to monitor all published data on an ongoing basis to ensure it is accurate and complete
- ensure any out of date or incorrect information identified is updated as soon as possible and in any event within one month

## Glossary and legal references

[Glossary](#)

[Legal references](#)

## Related content

[Publishing scheme information](#)

# The governing body

- The governing body is responsible for running a scheme
- It may be the trustees or managers of an occupational pension scheme
- In a public service pension scheme it is the scheme manager
- PS governance needs to take into account the differing responsibilities of the scheme manager, pension board and, where appropriate, pension committee
- Each PS scheme should determine who fulfils the role of scheme manager according to their regulations and local arrangements
- The code also sets out expectations for the pension board in their role

# Increased importance: Internal controls

- Internal controls are the policies, processes and procedures carried out in running the scheme
- Governing bodies may delegate operational tasks but they retain accountability
- Several modules within the new code focus on risk management and specific controls that should be in place
- The modules set out below contain systems, arrangements or procedures that governing bodies should have in place

Internal controls	Administration and management
<ul style="list-style-type: none"> <li>• Identifying, evaluating and recording risks</li> <li>• Internal controls</li> <li>• Assurance reports on internal controls</li> <li>• Scheme continuity planning</li> <li>• Risk management function</li> </ul>	<ul style="list-style-type: none"> <li>• Financial transactions</li> <li>• Record keeping</li> <li>• Data monitoring and improvement</li> <li>• Receiving contributions</li> <li>• Monitoring contributions</li> <li>• Maintenance of IT systems</li> <li>• Cyber controls</li> </ul>

# New Elements: ESOG & ORA

- Most private sector schemes have to have and operate an Effective System of Governance
- The elements of an ESOG includes the processes and procedures in around half the code
- In place now (technically)
- Most private sector schemes with 100 or more members must complete an Own Risk Assessment
- The ORA is a regular process where the governing body assesses the effectiveness and risks of the ESOG
- Regulations set out frequency
- Code sets out content and approach

These slides remain the property of The Pensions Regulator and their content should not be altered on reproduction.

# Consultation

- Consulted between 17 March and 26 May 2021
- Spoke with over 1,000 members of the pensions community
- Received 103 formal responses
- Nearly 17,400 individual answers to questions
- Meaningful consideration given to responses
- Design and content changes

# When?

- Coming into force soon
- Currently in final approval process
- Needs to sit in Parliament for 40 days
- Will be widely publicised
- Familiarise yourself with the draft

<https://www.thepensionsregulator.gov.uk/en/document-library/code-of-practice>

# Questions



**Thank you for coming!**

**Day two: Bevin Hall 10:00**

[bluelightpensions@local.gov.uk](mailto:bluelightpensions@local.gov.uk)

[www.fpsboard.org](http://www.fpsboard.org)

[www.fpsregs.org](http://www.fpsregs.org)

[www.fpsmember.org](http://www.fpsmember.org)