Public Service Pension

Employers

Staffordshire Pension Scheme

Employers meeting

Andy Nicholls
Industry liaison manager

25 June 2019

The Pensions Regulator

Making workplace pensions work

The information we provide is for guidance only and should not be taken as a definitive interpretation of the law.

DM 6469907 vl2 These slides remain the property of The Pensions Regulator and their content should not be altered on reproduction.

The Pensions Regulator

E

Agenda

- Our role, responsibilities and powers
- Your role and responsibilities
- Our expectations
- The importance of good data
- Scheme returns
- Reporting a breach
- Lessons from casework
- Data related initiatives: GDPR, pensions dashboard
- The need for cyber resilience

Be ScamSmart

The FCA and TPR have launched a joint TV advertising campaign to raise awareness of pension scams and the most common tactics used by fraudsters.

New statistics show that pension scam victims lose over £90,000 each on average.

A cold calling ban is in force

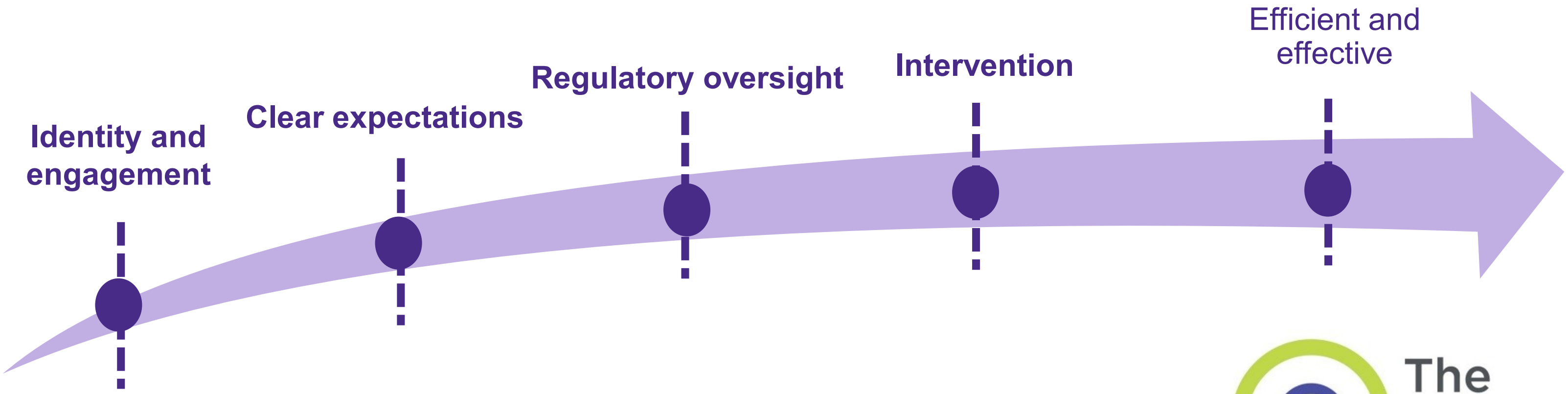
Print out and include the pension scams guide in your user documents (eg annual member statements and transfer packs).

Find out more at: www.tpr.gov.uk/pension-scams

The Pensions Regulator

The Pensions Regulator

- Our role is to protect workplace pensions
- We are being **clearer, quicker and tougher**
- We are changing in five key areas:
  - clarifying our identity
  - setting clear expectations
  - improving our regulatory oversight
  - using a wider range of regulatory interventions
  - being more efficient and effective



Driving compliance through supervision

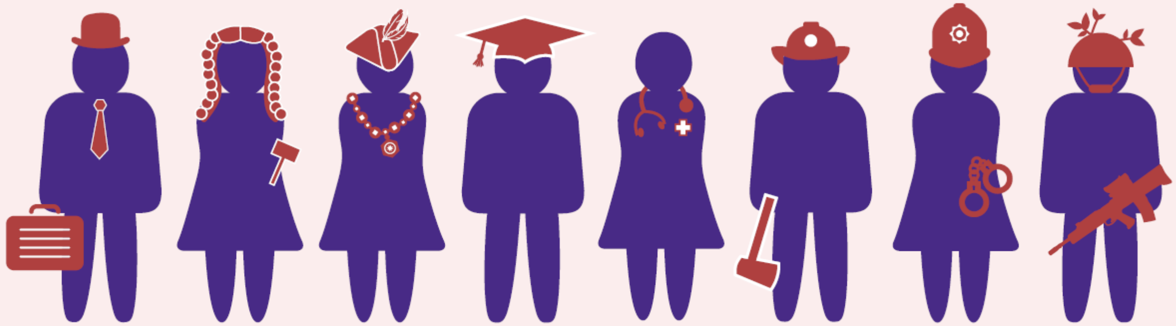
- One-to-one supervision is part of our evolving approach to protecting and regulating pensions
- www.tpr.gov.uk/regulate-and-enforce/one-to-one-supervision.aspx

The Pensions Regulator

Introduction

- We regulate the governance and administration of public service pension schemes, which provide pensions for civil servants, the judiciary, local government, teachers, health service workers, members of fire and rescue services, members of police forces and members of the armed forces
- Our Code of Practice 14 sets out the standards of conduct and practice we expect

8 workforces



16.5 million memberships

24,000 employers

Our roles and responsibilities

- We regulate compliance with the Governance and Administration requirements introduced by the Public Service Pensions Act 2013:
  - we engage mainly with scheme managers and pension boards
  - investment: not the what (compliance with investment regulations) but the how (investment governance) - LGPS only
    - ➢ www.tpr.gov.uk/guidance/db-investment.aspx
- To educate and enable:
  - codes, toolkit, news-by-email
    - ➢ www.tpr.gov.uk/doc-library/codes.aspx
    - ➢ https://trusteetoolkit.thepensionsregulator.gov.uk/
    - ➢ https://forms.thepensionsregulator.gov.uk/news-by-email/subscribe
- To enforce:
  - improvement and third party notices, fines etc

Our regulatory powers

- Appoint a skilled person to assist the pension board
- Civil penalties – up to £5,000 to an individual or £50,000 to a corporate body
- Collect data through the scheme return
- Criminal prosecution
- Improvement notices and third party notices – require specific action to be taken within a certain time
- Information – require any relevant person to produce any relevant document or information
- Inspection – at own premises and/or premises of a third party
- Publish reports about a case (which might include naming those at fault)
- Recover unpaid contributions from employers on behalf of the scheme manager
- Report misappropriation – notify the scheme manager about pension board conflicts or misuse regarding assets
- Skilled person report – require scheme managers to provide a report made by a skilled person nominated by the regulator

TPR focus 2018

- Ongoing risk assessment and intelligence gathering
  - www.tpr.gov.uk/docs/public-service-research-2018.pdf
- Key focus areas:
  - record-keeping and data quality

We have changed as a regulator; we are being **clearer** with those we regulate, **quicker** to act where our expectations are not being met - and **tougher** on employers that do not comply with their duties and trustees who do not act in the interests of their members.

2017 survey

- 191 of the 207 public service pension schemes completed the survey (92% covering 98% of all memberships)
  - This compares to a response rate of 90% in 2016, 48% in 2015 and 53% in 2013

Scheme type	Interviews	Schemes		Memberships[1]	
		Universe	Survey coverage	Universe	Survey coverage
Other	11	11	100%	9,978,735	100%
Firefighters	49	50	98%	114,024	97%
Local Government	88	100	88%	6,246,498	94%
Police	43	46	93%	372,312	97%
Total	**191**	**207**	**92%**	**16,711,569**	**98%**

Employer legal responsibilities - England and Wales

Regulation 80 of the LGPS (England and Wales) regulations 2013 states:

- A scheme employer '*must give that authority such other information as it requires for discharging its scheme functions*' and
- '*Within three months of the end of each scheme year, each scheme employer must give a statement to the appropriate administering authority giving the following details in respect of each employee who has been an* ***active member*** *during the scheme year*':
  - the employee's name, gender, date of birth, NI number, unique reference number relating to each employment
  - the dates of active membership
  - pensionable pay received and employee contribution deducted
  - any employer contribution in relation to the employee's pensionable pay
  - any additional employee or employer contributions
  - ➢ www.lgpsregs.org/schemeregs/lgpsregs2013/timeline.php#r80

Our expectation - employer responsibilites

Two way engagement approach:

- Employers:
  - required to provide information requested
  - have awareness of terms of employer agreements
  - abide by contract terms / obligations under regulations
  - manage HR / payroll systems
  - provide quality data (eg member joiner and leaver forms)
  - report a material breach of law
- Scheme managers:
  - follow scheme regulations, rules and requirements
  - have awareness of terms of employer agreements
  - have clear, robust, published processes / deadlines / communications
  - designate a scheme contact point
  - follow through on non compliance
  - understand material breach of law reporting requirements

Local pension boards

Pension boards are responsible for assisting the scheme manager in securing compliance with:

- scheme regulations
- other governance and administration legislation
- any requirements of The Pensions Regulator
- additional matters, if specified by scheme regulations
- pension boards need to have an equal number of employer representatives and member representatives (they may also have other types of members, such as independent experts).

- For simple guides to pension boards:
- www.tpr.gov.uk/public-service-schemes/pension-guides.aspx#s18403

Record keeping

- Good record keeping is a key part to the successful running of a scheme and allows schemes to meet their legal obligations
- We know from engagement that standards vary widely, and some schemes do not prioritise this appropriately, so TPR expects:
  - scheme managers to engage with administrators over service and security
  - assess data and put in place a plan to address issues
- Guidance on developing an improvement plan:
  - ➢ www.tpr.gov.uk/docs/improve-data-guide.pdf

Improving your data

- Scheme managers should undertake an **annual** data review and put in place an improvement plan where they identify issues - data improvement is a continuous process, not a one-off exercise
- Our quick guide (www.tpr.gov.uk/docs/improve-data-guide.pdf) can help you design a plan or assess an existing one
- Poor data integrity has a real impact on members - accurate records are key to ensuring:
  - the right members get the right benefits at the right time,
  - accurate valuations and calculation of the cost cap
- The data needed to run an efficient and effective scheme should be checked regularly – both 'common data' (applicable to all schemes) and 'conditional data' (dependent on scheme type, structure and system design) (www.tpr.gov.uk/docs/measure-data-guide.pdf)
- Data should be well managed day to day to ensure it is accurate and complete
- Though administrators may look after records on a day to day basis, scheme managers are still accountable

The Pensions Regulator

Record keeping - survey results

Most schemes have conducted a data review in the last year

Last data review
75% in last 12 months
15% longer ago
2% never
8% don’t know

Almost two-thirds identified issues in their latest review

Identified issues
62% identified issues
25% no issues identified
3% don’t know if issues
10% not reviewed (inc. DK)

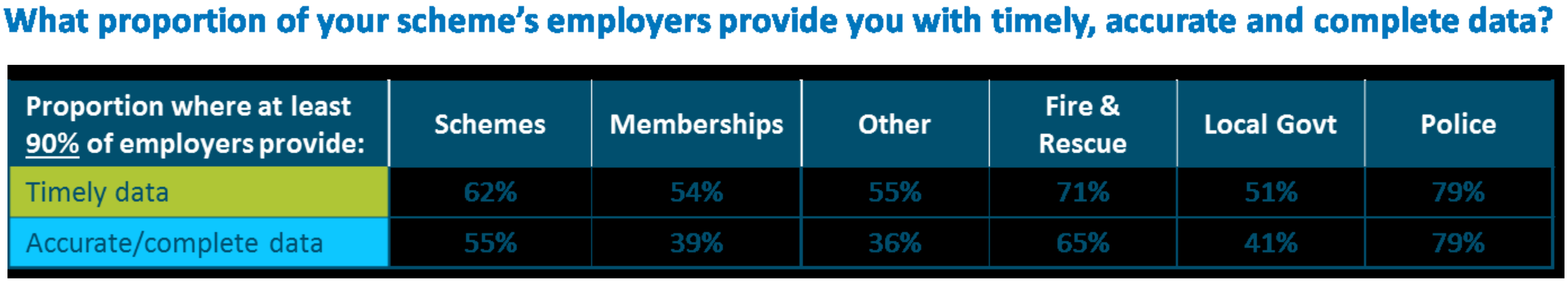
In most cases data rectification is in progress but not complete

Data improvement plans
19% data improvement plan
43% no data improvement plan
28% no issues identified (inc. DK)
10% not reviewed (inc. DK)

Many schemes are doing an annual data review, but take up of data improvement plans is low. Decrease in LGPS carrying out a data review and employer data is a bigger concern than for other schemes.

Record keeping - overview

- We consider 90% of employers providing good quality data to be an important threshold
- 62% of all schemes reported that that at least 90% of their employers provided **timely data**
- And 55% of all schemes reported that at least 90% of their employers provided **accurate and complete data**



What proportion of your scheme's employers provide you with timely, accurate and complete data?

Proportion where at least 90% of employers provide:	Schemes	Memberships	Other	Fire & Rescue	Local Govt	Police
Timely data	62%	54%	55%	71%	51%	79%
Accurate/complete data	55%	39%	36%	65%	41%	79%

All respondents **(Base, Don't know, Did not answer question**) - Schemes (191, 9-12%, 2%), Memberships (191, 2- 14%, 0%), Other (11, 0-18%, 0%), Fire (49, 20-22%, 2%), **LG (88, 6-7%, 0%),** Police (43, 7-9%, 7%)

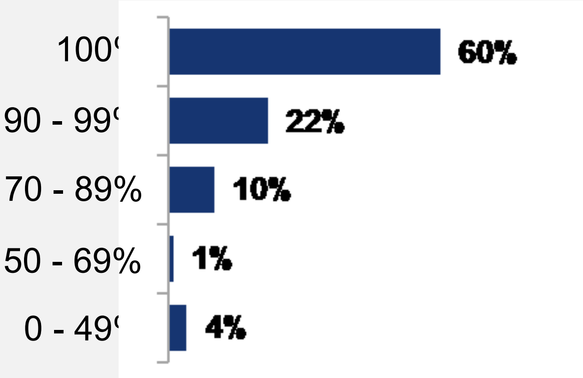
In LGPS, the proportion of schemes that did **NOT** report that that at least 90% of their employers provided timely data was **53%*** - and **62%*** did **NOT** report 90%+ accurate and complete data (*includes 7% of LGPS schemes that didn't know).

Scheme return requirements 2018

- From 2018 will be asked to report on:
  - when scheme last measured common data
  - common data score
  - when scheme last measured scheme specific (conditional) data
  - scheme specific data score
- This will help us understand and segment the landscape and target interventions / track progress
- Common data = data used to identify members (eg DOB, NINO, name)
- Scheme specific data = other data needed to run the scheme:
  - in public service schemes this includes data required by the regulations, data needed for valuation, compliance with scheme regulations etc
- This change for public service schemes may require systems and process changes (www.tpr.gov.uk/docs/measure-data-guide.pdf)
- For more information on the scheme return www.tpr.gov.uk/public-service-schemes/reporting-duties.aspx

Member communications - survey

Proportion of active members receiving annual benefit statement by statutory deadline



Mean % receiving by deadline	
2017 survey	93%
2016 survey	75%

- Significant improvements over the last year
- 60% of schemes reported that all members received their ABS on time (up from 43% in 2016)
- The mean was 93% (up from 75% in 2016)

In LGPS 45% of schemes reported that 100% of members received their ABS by the statutory deadline

Reporting breaches of law

- Legal duty to report a breach of the law that is likely of material significance to TPR for:
  - scheme manager
  - pension board member
  - professional advisers
  - employers
  - administrators and others providing advice to the manager
- Reporters to determine if a breach has occurred based on reasonable cause and not a mere suspicion
- TPR provides example scenarios and RAG system for assessing scale of materiality by way of:
  - cause
  - effect
  - reaction
  - wider implications

➢ www.tpr.gov.uk/docs/PS-reporting-breaches-examples-traffic-light-framework.pdf

Breaches of law reports - Teachers' Pension Scheme

- 2 breach of law reports were received in 2016 from an administrator
- 43 employers were failing to submit their End of Year Certificates (EOYCs) to the scheme manager by the legal deadline
- The administrator had made multiple contacts with each employer
- Our engagement:
  - we engaged with the non-compliant employers
  - the engagement identified a lack of knowledge and understanding by employers on EOYC submissions
  - all but one employer is now compliant
  - the scheme manager removed the final employer from the scheme (the employer has now gone insolvent)
- For more detail:
  - ➢ www.tpr.gov.uk/docs/regulatory-intervention-section-89-teachers.pdf

Public service pension scheme fined £1000

- We issued a £1,000 fine against the London Borough of Barnet scheme manager for failing to submit its 2016 scheme return:
  - we issued a scheme return notice to the scheme manager on 9 July 2016, requesting the scheme return be submitted by 12 August
  - the return was not received and further communications from TPR not replied to
  - so the matter was referred to TPR's Determinations Panel on 24 February 2017
  - the penalty notice was issued to the scheme manager on 13 April and paid on 9 June

Different use of powers - update

- In 2018, we used a number of different powers for the first time
- **Production orders** - require institutions to hand over evidentially admissible financial information on individuals or organisations under the **Proceeds of Crime Act 2002**, were used successfully as part of an investigation into pension fraud:
  - we required a bank to hand over statements and other details of the accounts linked to the trustees of a pension scheme
- We fined a trustee that **failed to complete** a **valuation on its DB pension** scheme, using our power under section 10 of the Pensions Act 1995:
  - the trustee was ordered to pay a **£25,000** fine after it twice failed to have the scheme valuation completed (required every three years)
- And we prosecuted a recruitment company, its directors and a number of its senior staff after they worked together to illegally opt-out workers who had been automatically enrolled into a workplace pension scheme
  - we **criminally prosecuted** under the **Computer Misuse Act 1990**

Use of powers – some more cases

- Accountant who was also trustee and administrator – custodial sentence received for fraudulently taking more than £290,000 from scheme. We are pursuing recovery of the money
- Professional trustee firm fined £103,750 for breaching multiple areas of pensions law - failing to obtain audited accounts for the scheme for 4 years, failing to give members statutory money purchase illustrations (SMPIs) for 2 years and not reporting these breaches to us
- Accounts manager submitted false automatic enrolment declarations of compliance. Investigation found he hadn't enrolled staff. They were fined £5000

What does this mean in practice

- Make sure there are appropriate internal controls:
  - service level agreements are set up, even with in-house administrators
  - there are processes to receive, check and review data
  - and processes around the Data Protection Act and data breaches
    - more guidance coming from us
- Data to be reviewed:
  - annually and on triggering events (new administrator)
  - common / scheme specific data
  - the review is robust
- Robust data improvement plans:
  - new guidance coming from TPR

TPR and Public Service schemes

- Governance and administration
  - knowledge and understanding of board members, risk register, cyber security, quarterly pension board meetings, data quality, scheme returns…
- Data quality
  - Annual reviews
  - Common and scheme specific data, their scores and improvement plans
- Member communications
  - Annual Benefit Statements – accurate and timely
  - Scams
- Automation – data collection
  - paper v electronic
  - monthly v annual
- Pensions Dashboard

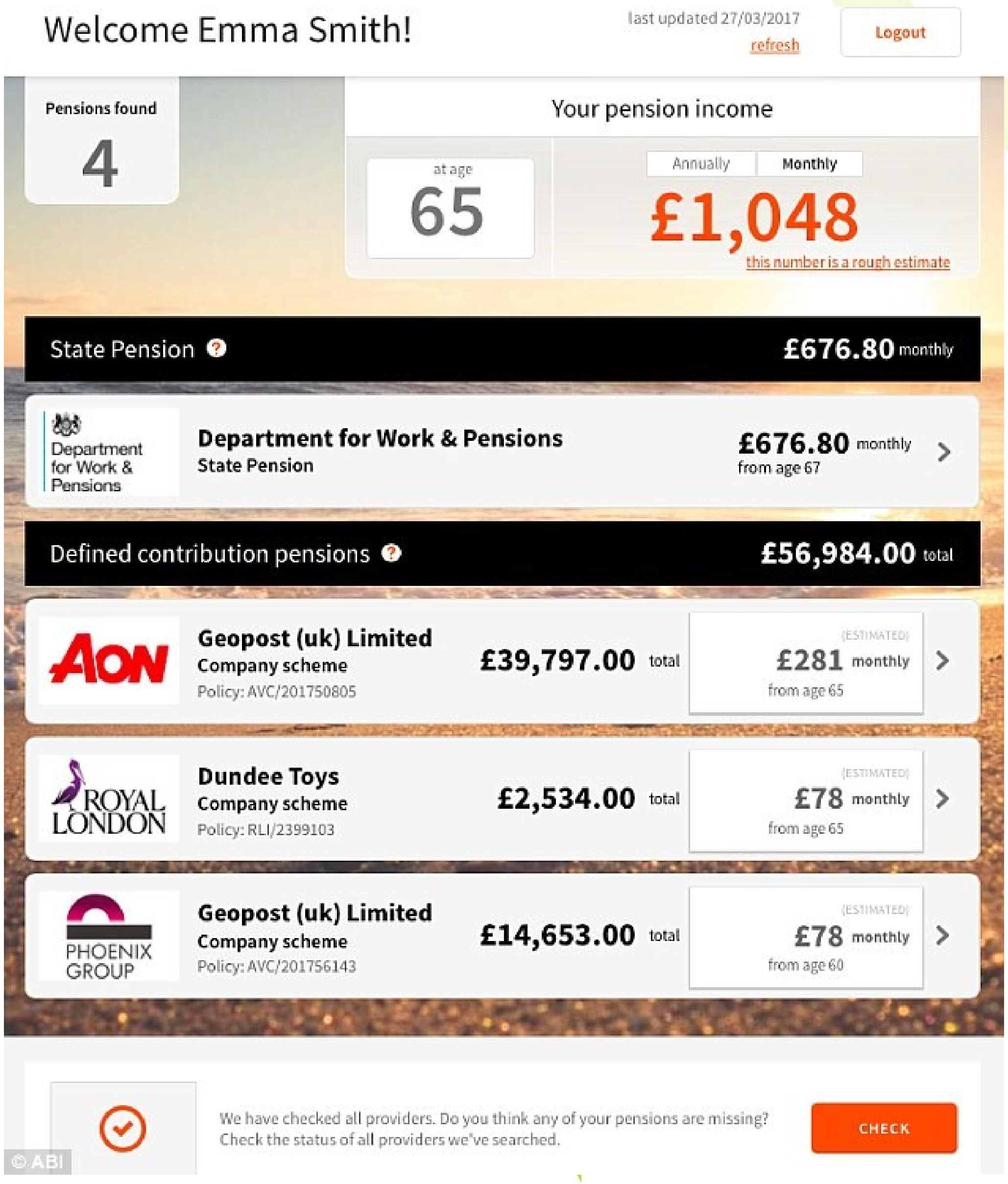
The Pensions Regulator

What are the challenges facing pension schemes

- Member engagement:
  - online access
- Enhanced requirements:
  - increased reporting requirements
  - pensions dashboard (might become a legal requirement to provide member benefit data)
  - cyber security

Pensions dashboard

- Money and Pensions Service
- Industry Delivery Group appointments (Chris Curry principal), industry representatives etc
- Legislation required
- All pension schemes?
- Live by?
- Phasing?
- Data standards
- Data display
- Architecture
- etc
- **Employer's role?**



Welcome Emma Smith!

last updated 27/03/2017
refresh

Logout

Pensions found
4

Your pension income

at age
65

Annually | Monthly

£1,048
this number is a rough estimate

State Pension ? £676.80 monthly

Department for Work & Pensions
State Pension
£676.80 monthly
from age 67

Defined contribution pensions ? £56,984.00 total

Geopost (uk) Limited
Company scheme
Policy: AVC/201750805
£39,797.00 total
(ESTIMATED) £281 monthly
from age 65

Dundee Toys
Company scheme
Policy: RLI/2399103
£2,534.00 total
(ESTIMATED) £78 monthly
from age 65

Geopost (uk) Limited
Company scheme
Policy: AVC/201756143
£14,653.00 total
(ESTIMATED) £78 monthly
from age 60

We have checked all providers. Do you think any of your pensions are missing?
Check the status of all providers we've searched.

CHECK

© ABI

Cyber resilience in pensions schemes

- Pension schemes are potentially valuable targets for fraudsters as they hold large amounts of personal information
- Scheme managers are responsible for putting in place controls to ensure the security of data and assets
- TPR CEO has said that cyber security should be on risk registers
- Not just an administrator problem – (eg what controls are around the data shared with the scheme actuary, legal advisors and pension board)
- Not just about cyber 'defence' but cyber resilience:
  - look at systems, processes and people (access and training) to reduce the risk
  - prepare for when things go wrong – how to recover data, how to report internally and externally (members, ICO, TPR)

Mitigation against cyber threats

- Most cyber attacks exploit basic weaknesses in software and IT systems
- Our guidance to trustees and scheme managers on principles for building cyber resilience:

  www.tpr.gov.uk/guidance/cyber-security-principles-for-pension-schemes.aspx

- Government estimates that 80% of breaches could be prevented by following these 10 steps from the National Cyber Security Centre (part of GCHQ):

  www.ncsc.gov.uk/guidance/10-steps-executive-summary

- Cyber Essentials is a Government-backed, industry-supported scheme to help organisations protect themselves against the most common threats found on the internet. It shows you how to fix basic weaknesses and get a good level of cyber security in place.

  www.cyberaware.gov.uk/cyberessentials

Summary

- Our key focus areas are record-keeping and data quality
- Employers must provide accurate and timely data for record keeping
- Data quality to be continuously reviewed:
  - the reviews are sufficiently comprehensive
  - and robust data improvement plans are in place and progressed
- Good governance and administration - make sure there are appropriate controls:
  - service level agreements are set up, even with in-house administrators
  - report breaches of the law when appropriate
- Additional scheme return requirements this year – result ssoon
- Scheme managers are responsible for having controls for cyber resilience
- Outsourcing does **not** reduce or remove a scheme manager's responsibility or accountability

Automatic enrolment what's happened so far …

- As at the end of **May 2019**
  - **1,506,234** employers have completed their **declaration of compliance,**
  - covering **31.5m** workers, of which:
    - **11.6m** (37%) were already in a qualifying scheme;
    - **10m** people (32%) were automatically enrolled;
    - 439k (1%) workers had the transitional period applied;
    - and 9.4m (30%) were 'none of the above'.
  - **154,719** employers have completed a **re-declaration of compliance**
    - **636,000** workers have been re-enrolled

Automatic enrolment - use of powers

- Some of our powers used
  (to 31 March 2019):
  - 875 information notices
  - 1,631 statutory inspection notices
  - 153,080 compliance notices
  - 26,235 unpaid contribution notices
  - 80,385 fixed penalty notices
  - 21,520 escalating penalty notices (EPN)
- We publish details of those that have:
  - paid their EPN, but remain non-compliant; or
  - failed to pay their EPN and are subject to a court order

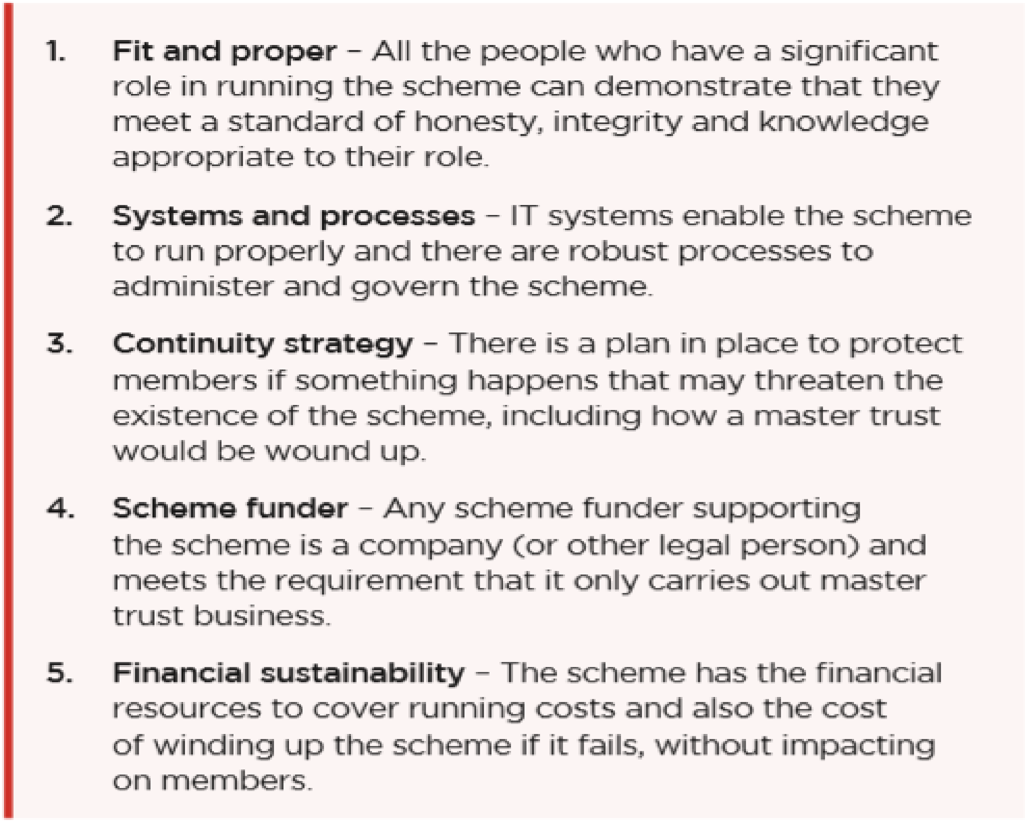
➢www.tpr.gov.uk/doc-library/escalating-penalty-notices.aspx

283,804 cases closed by
31 March 2019

The Pensions Regulator

Master Trust authorisation

Five areas:



1. **Fit and proper** – All the people who have a significant role in running the scheme can demonstrate that they meet a standard of honesty, integrity and knowledge appropriate to their role.
2. **Systems and processes** – IT systems enable the scheme to run properly and there are robust processes to administer and govern the scheme.
3. **Continuity strategy** – There is a plan in place to protect members if something happens that may threaten the existence of the scheme, including how a master trust would be wound up.
4. **Scheme funder** – Any scheme funder supporting the scheme is a company (or other legal person) and meets the requirement that it only carries out master trust business.
5. **Financial sustainability** – The scheme has the financial resources to cover running costs and also the cost of winding up the scheme if it fails, without impacting on members.

Master Trust authorisation

- **As at 30 April 2019**

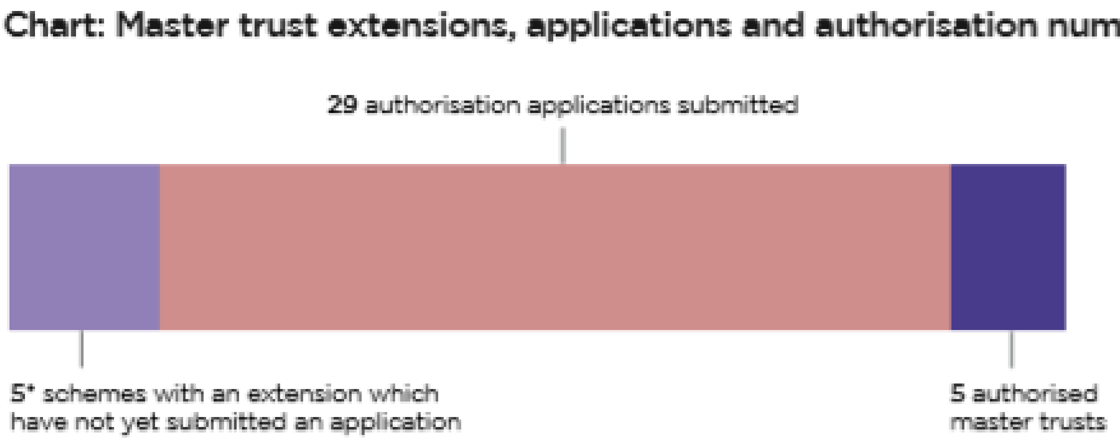


Chart: Master trust extensions, applications and authorisation numbers

  - **9 have exited the market**
  - **35 have notified us that they will be exiting**

- **Impact on payroll?**

Useful tools, checklists and guidance - (i)

- **Annual benefits statement -** www.tpr.gov.uk/docs/public-service-annual-benefit-statements-guide.pdf www.tpr.gov.uk/docs/public-service-annual-benefits-statement-checklist.pdf www.tpr.gov.uk/docs/PS-guide-key-information-to-provide-to-members.pdf
- **Data measuring guidance -** www.tpr.gov.uk/docs/measure-data-guide.pdf
- **GDPR guidance - Information Commissioner's Office (ICO) -** https://ico.org.uk/for-organisations/guidance-index/
- **Improvement plan guidance -** www.tpr.gov.uk/docs/improve-data-guide.pdf
- **Internal controls checklist -** www.tpr.gov.uk/docs/public-service-internal-controls-checklist.pdf

Useful tools, checklists and guidance - (ii)

- **Public service - scheme self assessment toolkit -** www.tpr.gov.uk/public-service-schemes/assess-your-scheme.aspx
- **Public service - personal self assessment tool -** https://education.thepensionsregulator.gov.uk/login/index.php
- **Reporting a breach -** www.tpr.gov.uk/docs/PS-reporting-breaches-examples-traffic-light-framework.pdf
- **Risk register example -** www.tpr.gov.uk/docs/public-service-example-risk-register.pdf
- **Scheme return -** www.tpr.gov.uk/public-service-schemes/reporting-duties.aspx
- **Trustee Toolkit -** https://trusteetoolkit.thepensionsregulator.gov.uk/

Useful links

- **Our website -** www.tpr.gov.uk/
- **Codes -** www.tpr.gov.uk/doc-library/codes.aspx
- **Code of practice 14 - Governance and administration of public service pension schemes -** www.tpr.gov.uk/public-service-schemes/code-of-practice.aspx
- **Governance -** www.tpr.gov.uk/21c-trustee
- **Latest research -** www.tpr.gov.uk/public-service-schemes/research-and-analysis.aspx
- **NAO report -** www.tpr.gov.uk/docs/vfm-review.pdf
- **Pension scams -** www.tpr.gov.uk/pension-scams.aspx
- **Public service area -** www.tpr.gov.uk/public-service-schemes.aspx
- **TPR Future -** www.tpr.gov.uk/about-us/protecting-workplace-pensions.aspx

Thank you

We are here to help!

Request a guest speaker:
https://secure.thepensionsregulator.gov.uk/speaker-request.aspx

Contact us at:
www.tpr.gov.uk/contact-us.aspx

Subscribe to our news by email:
https://forms.thepensionsregulator.gov.uk/subscribe.aspx

The information we provide is for guidance only and should not be taken as a definitive interpretation of the law.

DM 6034372 v3I These slides remain the property of The Pensions Regulator and their content should not be altered on reproduction.

The Pensions Regulator

Additional slides

National Cyber Security Centre

What you can do to combat cyber attacks

Reducing The Impact

Most cyber attacks are composed of four stages: **Survey, Delivery, Breach and Affect.** The following **security controls,** applied at each stage of an attack, can reduce your organisation's exposure to a successful cyber attack.

Survey

User Education

Train all users to consider what they include in publicly available documents and web content. Users should also be aware of the risks from discussing work-related topics on social media, and the potential of being targeted by phishing attacks.

Who might be attacking you?

Cyber Criminals interested in making money through fraud or from the sale of valuable information.

Industrial competitors and foreign intelligence services interested in gaining an economic advantage for their companies or countries.

Hackers who find interfering with computer systems an enjoyable challenge.

Hacktivists who wish to attack companies for political or ideological motives.

Employees, or those who have legitimate access, either by accidental or deliberate misuse.

Delivery

Network Perimeter Defences

Can block insecure or unnecessary services, or only allow permitted websites to be accessed.

Malware Protection

Can block malicious emails and prevent mailware being downloaded from websites.

Password Policy

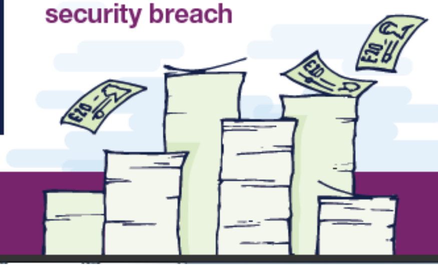
Can prevent users from selecting easily guessed passwords and locks accounts after a low number of failed attempts.

Secure Configuration

Restrict system functionality to the minimum needed for business operation, systematically apply to every device that is used to conduct business.

£600K-£1.15m

Average cost of security breach



Breach

Patch Management

Apply patches at the earliest possibility to limit exposure to known software vulnerabilities.

Monitoring

Monitor and analyse all network activity to identify any malicious or unusual activity.

Malware Protection

Malware protection within the internet gateway can detect malicious code in an important item.

Secure Configuration

Remove unnecessary software and default user accounts. Ensure default passwords are changed, and that automatic features that could activate malware are turned off.

User Access

Well maintained user access controls can restrict the applications, privileges and data that users can access.

User Training

User training is extremely valuable in reducing the likelihood of successful social engineering attacks.

Device Controls

Devices within the internal gateway should be used to prevent unauthorised access to critical services or inherently insecure services that may still be required internally.

Affect

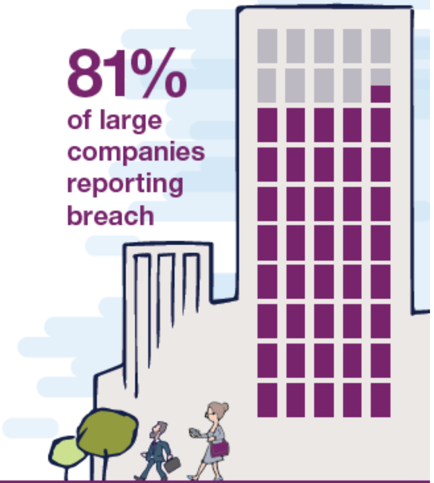
Controls For The Affect Stage

Once an attacker has achieved full access, it's much harder to detect their actions and eradicate their presence. This is where a more in-depth, holistic approach to cyber security can help.

10 Steps To Cyber Security outlines many of the features of a complete cyber risk management regime.

81%

of large companies reporting breach



National Cyber Security Centre

10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention

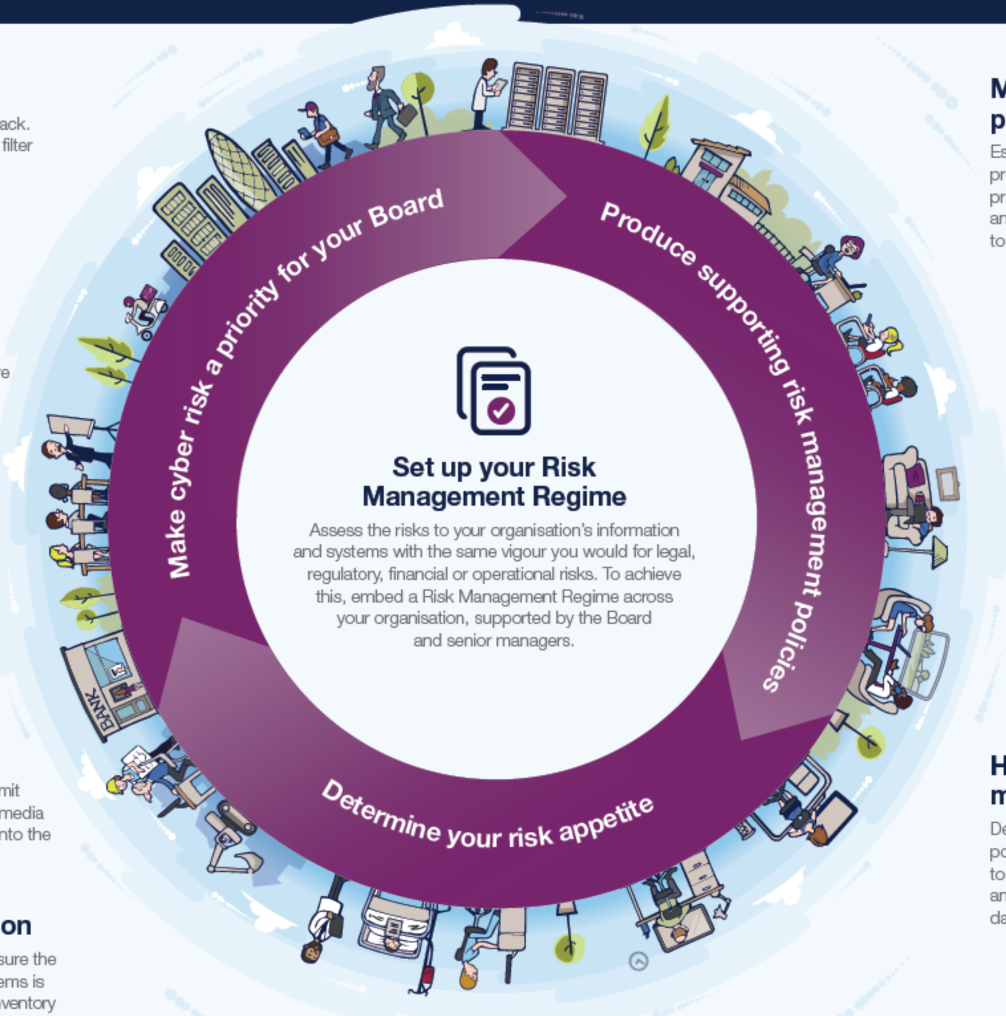
Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.



Make cyber risk a priority for your Board

Produce supporting risk management policies

Determine your risk appetite

Set up your Risk Management Regime

Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to www.ncsc.gov.uk @ncsc