



# Aon LGPS Cyber Scorecard

Summary report for:  
London Borough of Enfield Pension Fund

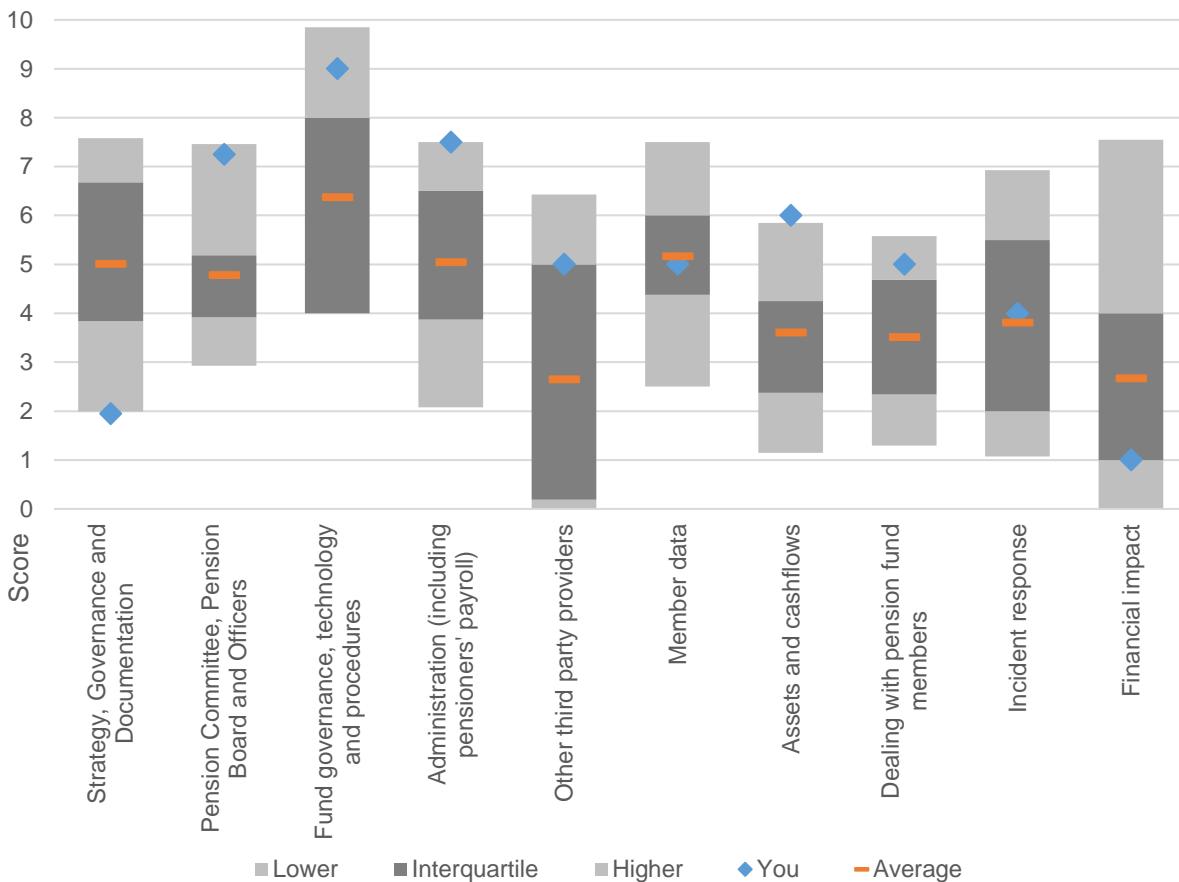
Based on responses by:  
Julie Barker

Date : 28 April 2021

The Aon LGPS Pension Cyber Scorecard is a high level assessment of the actions being taken by a LGPS administering authority in relation to cyber resilience. It is based on the results of around 50 multiple choice questions which have been completed for the fund.

The analysis below assesses your fund's cyber resilience measures in 10 areas, and also compares them against the steps being taken by other LGPS funds. The orange bar represents the average across all funds, while the grey areas represents the range between the 5th, 25th, 75th and 95th percentiles scores for each section. The blue diamond is your score.

In this basic assessment we have not provided any fund-specific commentary on your results, but would be happy to do so should that be helpful.



Your scores by section are summarised in the table below, which also shows the average score across the funds who have completed this assessment for comparison.

	Section scores (out of 10)		
	Your score	Average	
Strategy, Governance and Documentation	2.0	5.0	Lower
Pension Committee, Pension Board and Officers	7.3	4.8	Upper
Fund governance, technology and procedures	9.0	6.4	Upper
Administration (including pensioners' payroll)	7.5	5.0	Upper
Other third party providers	5.0	2.6	Upper
Member data	5.0	5.2	Interquartile
Assets and cashflows	6.0	3.6	Upper
Dealing with pension fund members	5.0	3.5	Upper
Incident response	4.0	3.8	Interquartile
Financial impact	1.0	2.7	Interquartile
<b>Overall score</b>	<b>51.7</b>	<b>42.6</b>	

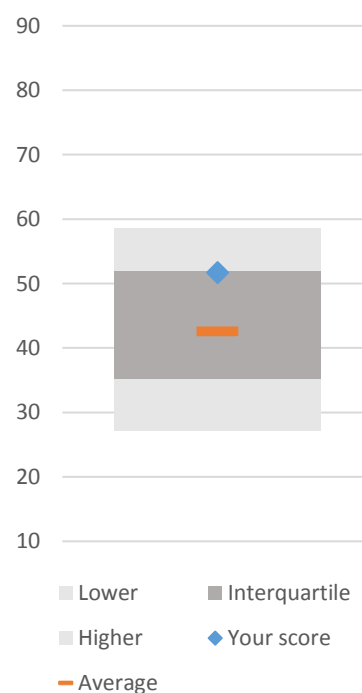
The scores in each section vary substantially between funds, with administering authorities focussing in different areas for a range of reasons. This assessment is intended to highlight areas of strength as well as areas of potential weakness.

In both the table and chart, "Lower" represents a result between the 5th and 25th percentile, "Upper" is a result between the 75th and 95th percentile, and "Interquartile" is between the 25th and 75th percentiles.

When considering your results, please note that a section score of 10 or a total score of 100 is a theoretical maximum which would only be achievable if all possible precautions were being taken.

It should also be noted that a high score does not guarantee your fund is secure. No pension scheme or organisation can be wholly protected from cyber risk, no matter how good the controls. However we hope that by considering this assessment administering authorities will identify actions they can take to protect the fund, the host authority, the participating employers and the fund members.

### Range of overall scores



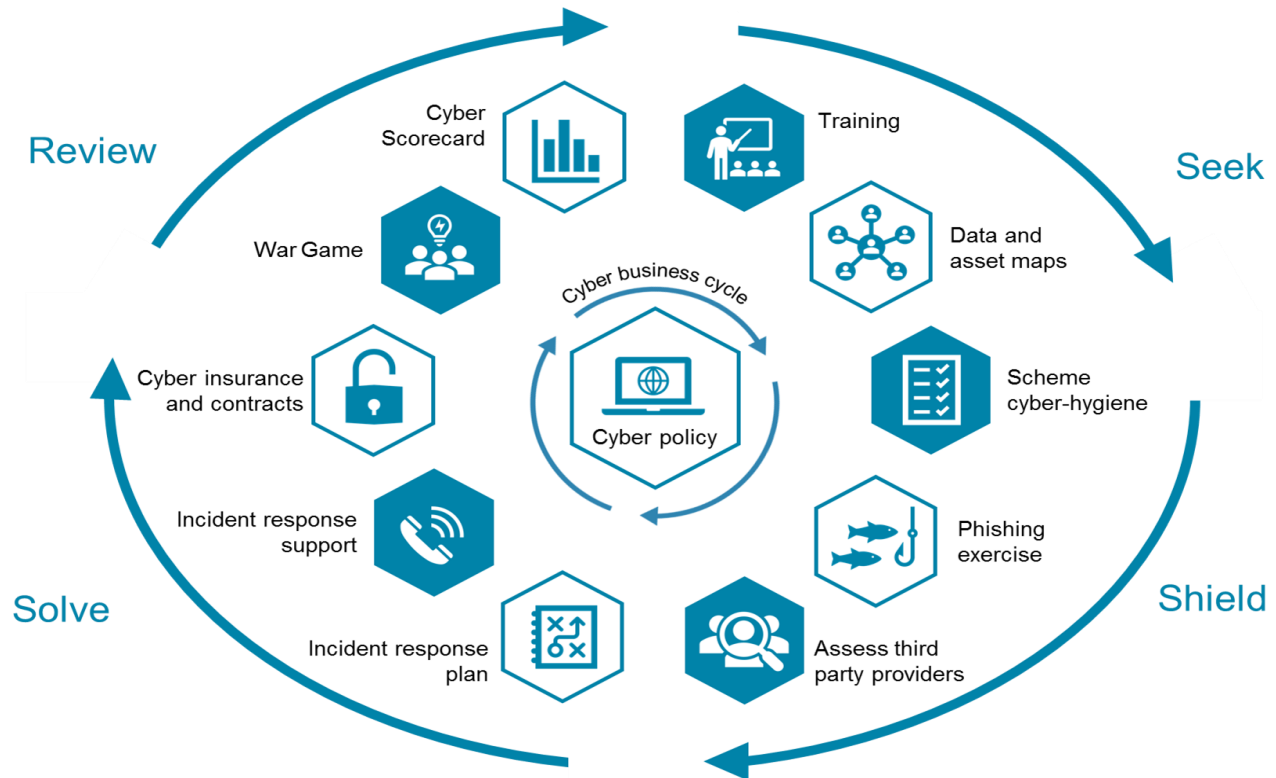
## Contacts

**Laura Caudwell**  
 Senior Consultant  
 +44 (0)117 948 5020  
[laura.caudwell@aon.com](mailto:laura.caudwell@aon.com)

**Jason Wilson**  
 Senior Consultant  
 +44 (0)207 086 4257  
[jason.wilson@aon.com](mailto:jason.wilson@aon.com)

## Aon's cyber solutions

Depending on your position there are a range of actions that pension schemes may want to take. Speak to us about our "Seek-Shield-Solve" framework and how we can support your pension scheme on its cyber journey.



## About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

### Copyright © 2021 Aon Solutions UK Limited. All rights reserved.

Aon Solutions UK Limited is authorised and regulated by the Financial Conduct Authority.

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. Consultants will be pleased to answer questions on its contents but cannot give individual financial advice. Individuals are recommended to seek independent financial advice in respect of their own personal circumstances.

Aon Solutions UK Limited is authorised and regulated by the Financial Conduct Authority.

Registered in England & Wales No. 4396810

Registered office: The Aon Centre | The Leadenhall Building | 122 Leadenhall Street | London | EC3V 4AN

[www.aon.com](http://www.aon.com)

# Appendix - How your answers compare

Over the following pages we have provided a summary of individual responses. These have not been amended in any way. If any of them need updating then we can do that easily.

**Your Response      Scorecard**

Q1.1 How have you assessed your cyber risks? (tick all that apply)

- We have not assessed our cyber risks
- We are currently in the process of assessing our fund cyber risks
- We have assessed the specific cyber risks that our fund is exposed to
- In assessing those risks we have consulted the Host Authority (Council)
- In assessing those risks we have consulted our key advisers and providers
- In assessing those risks we have consulted a cyber specialist

	4%
<b>Y</b>	46%
	58%
	79%
	42%
	13%

Q1.2 How is your Fund's cyber strategy developed and documented? (tick all that apply)

- We have not documented our Fund's cyber strategy
- We rely on our Host Authority's cyber strategy
- We have a Fund cyber policy document that captures our cyber strategy
- Our Fund cyber policy document has been reviewed in the past 24 months
- Our Fund cyber policy document has been developed in conjunction with the Council
- We had specialist cyber support when preparing our Fund's cyber policy document

	25%
<b>Y</b>	83%
	17%
	17%
	25%
	0%

Q1.3 For your Fund who has primary responsibility for cyber risk? (tick one)

- Chair of Committee
- All Committee members collectively
- Chief Finance Officer (i.e. Section 151 Officer in England)
- The Senior Pension Fund Officer (who is not the S151 Officer)
- Dedicated Cyber Officer or IT Officer from the Host Authority
- Providers
- We have not yet allocated primary responsibility
- Other – please specify

	0%
	4%
<b>Y</b>	21%
	29%
	17%
	0%
	21%
	8%

**Your  
Response      Scorecard**

Q1.4 Does the Pension Committee (or equivalent) receive updates on cyber risks, controls and incidents affecting the Fund?

- Yes – at every meeting
- Yes – usually at least once a year
- Yes – but generally less than once a year
- No

	33%
	21%
	17%
<b>Y</b>	29%

Q1.5 Does the Pension Board receive updates on cyber risks, controls and incidents affecting the Fund?

- Yes – at every meeting
- Yes – usually at least once a year
- Yes – but generally less than once a year
- No

	38%
	21%
	17%
<b>Y</b>	25%

Q1.6 How do your cyber risks link to your risk register? (tick all that apply)

- Cyber risks are not included in our risk register
- Cyber risks are included in our risks register
- The cyber risks in our risk register are reviewed at least once every 12 months
- We have reconsidered the information relating to our cyber risk on the risk register during 2020 due to the Covid-19 pandemic

	4%
<b>Y</b>	96%
	71%
	50%

Q2.1 Which of the following statements apply to your expectations of Pension Committee and Pension Board members and Pension Fund officers? (tick all that apply)

We expect them to not conduct pension fund business using a home/personal email account they use for normal life activities

We expect them to not conduct pension fund business on personal/shared IT devices unless they have password protection and up to date virus protection

They have clear guidance on the passwords they can use (e.g. guidance on length, structure and how frequent these should be changed)

They have clear guidance on how long they can retain Fund data and information, and how this can be securely destroyed (for example, what should retiring/leaving officers and Committee/Board members reaching the end of their term do with information)

We have a document for them which sets out the Fund's policies on the above and any other practices or behaviours which help individuals improve their own cyber security while conducting pension scheme business

	Your Response			Scorecard		
	Officers	PC Members	PB Members	Officers	PC Members	PB Members
We expect them to not conduct pension fund business using a home/personal email account they use for normal life activities	Y	Y	Y	100%	79%	33%
We expect them to not conduct pension fund business on personal/shared IT devices unless they have password protection and up to date virus protection	Y	Y	Y	88%	88%	54%
They have clear guidance on the passwords they can use (e.g. guidance on length, structure and how frequent these should be changed)	Y	Y	Y	100%	67%	25%
They have clear guidance on how long they can retain Fund data and information, and how this can be securely destroyed (for example, what should retiring/leaving officers and Committee/Board members reaching the end of their term do with information)	Y	Y	Y	88%	46%	17%
We have a document for them which sets out the Fund's policies on the above and any other practices or behaviours which help individuals improve their own cyber security while conducting pension scheme business	Y	Y	Y	58%	25%	13%

Q2.2 Which of the following statements apply to your officer and Committee/Board member training program? (tick all that apply)

- Our training program includes training on cyber risk at least annually
- Our training program includes training on cyber risk but less frequently than annually
- Our training program does not include training on cyber risk
- Our training includes specialist cyber resources as well as pension experts
- Our training on cyber risk is provided purely as part of the Host Authority's training

	Your Response			Scorecard		
	Officers	PC Members	PB Members	Officers	PC Members	PB Members
Our training program includes training on cyber risk at least annually	Y	Y	Y	63%	33%	33%
Our training program includes training on cyber risk but less frequently than annually				21%	25%	25%
Our training program does not include training on cyber risk				0%	13%	13%
Our training includes specialist cyber resources as well as pension experts				17%	8%	8%
Our training on cyber risk is provided purely as part of the Host Authority's training				46%	42%	21%

Q2.3 Which of the following best reflects your approach to managing the e-mail phishing risk? (tick one)

- Our Committee/Board members and officers have no specific training on phishing risks
- Some but not all of our Committee/Board members and officers are trained on phishing risk
- All of our Committee/Board members and officers are trained on phishing risks, including simulated phishing attacks
- I don't know

Y

4%
63%
13%
21%

**Your Response      Scorecard**

Q3.1 When sharing meeting papers and advice documents between Committee and/or Board members, which approaches are used? (tick all that apply)

Unencrypted email		42%
Email with encrypted attachment		8%
Other secure email facility or file sharing portal	Y	38%
Committee/Board portal (e.g. online meeting packs or Host Authority Committee portal)	Y	67%
Hard copy information via post		46%
Other - Please specify		8%

Q3.2 If you use a Committee/Board portal for scheme information, how and when was a security assessment last conducted on the portal? (tick one)

We have no portal		29%
No assessment undertaken		0%
External assessment but more than 24 months ago		0%
External assessment within last 24 months		0%
We rely on the provider/Host Authority to do checks on our behalf and we receive a report from time to time	Y	21%
We rely on the provider/Host Authority to do checks on our behalf but we don't get any reports on the findings or we don't know when the checks were last done		50%

Q3.3 Many Committees and/or Pension Boards and officers share Fund information in password-protected documents. If one of your officers, advisers or members left, in 12 months time would they be able to open your most recent documents? (tick one)

We never share Fund information in password-protected documents	Y	75%
Yes, our password is unlikely to have changed in that time		0%
Yes, although our password changes it follows the same structure (eg ABC2019! becomes ABC2020!)		0%
No, our password(s) change regularly and do not have a pattern		21%



**Your  
Response      Scorecard**

Q4.1 Is your day to day administration carried out in house, by a third party or shared services? (tick one)

Third party		8%
In house	Y	88%
Shared Services		4%
Other (please specify)		0%

Q4.2 How do you assess the cyber security of your main administration service and platform, whether in-house or outsourced (tick all that apply).

No assessment done		4%
Request provider's own standard cyber policy documents		58%
Fund-specific questionnaire		13%
Host Authority's cyber questionnaire for providers	Y	46%
Interview with provider		17%
Site visit		4%
Other (please specify)		17%

Q4.3 How regularly do you assess the administration provider and platform? (tick one)

Never		0%
At least annually	Y	42%
At least every 2 years		8%
Ad-hoc, no formal policy		46%
Other (please specify)		0%

Q4.4 Aside from obtaining cyber policy documents, which specific areas did your last assessment cover? (tick all that apply)

Adherence to published security standards	Y	63%
Details of network security and penetration testing	Y	83%
Detail of staff training and user access	Y	50%
Controls around transfer of data	Y	54%
Physical security provisions	Y	33%
Incident response planning	Y	67%
Other (please specify)		13%

**Your Response      Scorecard**

Q4.5 Was your last assessment done or supported by a cyber specialist (either external or from within the Host Authority)? (tick one)

- Yes
- No

<b>Y</b>	54%
	46%

Q4.6 Is your pensioners' payroll part of your main administration service and platform (i.e. rather than being processed by the Host Authority/Council's payroll service on your behalf)?

- Yes, and therefore the answers above apply to the pensioners' payroll too
- No, but the pensioners' payroll is subject to a cyber assessment at least annually
- No, but the pensioners' payroll is subject to a cyber assessment at least every 2 years
- No, but the pensioners' payroll is subject to a cyber assessment on an ad-hoc basis (no formal policy)
- No and the pensioners' payroll has not been subject to a cyber assessment
- No and I do not know if the pensioners' payroll has been subject to a cyber assessment
- Other (please specify)

<b>Y</b>	67%
	13%
	0%
	8%
	4%
	8%
	0%

**Your Response      Scorecard**

Q5.1 For which of the following Fund providers have you conducted a cyber security assessment in the last 24 months?  
(tick all that apply)

- Actuary
- Benefits Consultant
- Governance Consultant
- Investment Consultant
- Investment Managers
- Pooling Operator
- Custodian
- Lawyers
- External Auditors
- AVC providers
- Communications advisors
- Host Authority (e.g. Council)
- Other employers
- Tracing Service provider

	29%
	4%
	4%
	8%
	17%
	13%
	21%
	4%
	8%
	8%
	4%
Y	42%
	0%
	13%
	13%

Additional comments

Q5.2 Which of the following approaches do you use when assessing the cyber security of your non-administration providers?  
(tick all that apply)

- No assessments done
- Request provider's own standard cyber policy documents
- Fund-specific questionnaire
- Council's cyber questionnaire for suppliers
- Interview with provider
- Site visit
- Other (please specify)

	54%
	38%
	8%
Y	25%
	8%
	0%
	4%

Additional comments

**Your  
Response      Scorecard**

Q5.3. How regularly do you typically assess your non-administration providers? (tick all that apply if it differs for different providers and please provide details)

Never		42%
At least annually	Y	13%
At least every 2 years		4%
Ad-hoc, no formal policy		29%
Other (please specify)		13%

Additional comments

Q5.4 Aside from obtaining cyber policy documents, which specific areas do your assessments typically cover? (tick all that apply)

Adherence to published security standards	Y	46%
Details of network security and penetration testing	Y	50%
Detail of staff training and user access	Y	33%
Controls around transfer of data	Y	50%
Physical security provisions	Y	21%
Incident response planning	Y	29%
Other (please specify)		8%

Additional comments

Q5.5 Was your last assessment done or supported by a cyber specialist (either external or from within the Host Authority)? (tick one)

Yes	Y	38%
No		58%

**Your Response      Scorecard**

Q6.1 Which best describes your understanding of the scheme member data flows in your Fund? (tick one)

- We have not yet considered where/how the data flows
- We understand the main data flows and have documented these but it is not comprehensive
- We have a comprehensive data map which documents all of the places that our member data is used and transferred

	21%
	67%
<b>Y</b>	13%

Q6.2 Which of the following approaches are used to transfer individual scheme member data between employers and officers? (tick all that apply)

- Unencrypted email
- Email with encrypted attachment
- Other secure email or file sharing portal
- Hard copy information via post (e.g. leaver forms)
- Other (please specify)

<b>Y</b>	25%
<b>Y</b>	67%
<b>Y</b>	92%
	50%
	8%

Q6.3 Which of the following security measures are in use across bulk data transfers of scheme member data from/to employers? (tick all that apply)

- Unencrypted email
- Email with encrypted attachment
- Other secure email
- File sharing portal e.g. secure employer data upload site
- Other (please specify)

	4%
<b>Y</b>	67%
<b>Y</b>	58%
	75%
	8%

Q6.4 If you have an employer data portal, have you conducted a security assessment of it (where they upload scheme member data)? (tick one)

- We have no employer data portal
- No assessment undertaken
- External assessment but more than 24 months ago
- External assessment within last 24 months
- We rely on the provider to do checks on our behalf and we receive a report from time to time
- We rely on the provider to do checks on our behalf but we don't get any reports on the findings or we don't know when the checks were last done

<b>Y</b>	25%
	0%
	0%
	25%
	25%
	25%

**Your Response      Scorecard**

Q6.5 Which of the following approaches are used to transfer individual scheme member data between providers and/or other organisations (e.g. solicitors or other pension schemes) and/or officers? (tick all that apply)

Unencrypted email		8%
Email with encrypted attachment	Y	79%
Other secure email or file sharing portal	Y	83%
Hard copy information via post (e.g. leaver forms)		46%
Other (please specify)		0%

Additional comments

Q6.6 Which of the following security measures are in use across all other bulk scheme member data transfers e.g. between third party administrators, actuaries and/or fund officers? (tick all that apply)

Unencrypted email		8%
Email with encrypted attachment	Y	58%
Other secure email or file sharing portal	Y	88%
Other (please specify)		4%

Additional comments

Q6.7 Does your bulk data leave your providers to go to third party subcontractors (e.g. third-party administrator sends benefit statement data to a sub-contracted printing firm, software provider shares data with a sub-contractor for disaster recovery purposes)? (tick one)

No	Y	38%
We don't know		4%
Yes, but we don't have any insight into the controls		13%
Yes, and we are comfortable that suitable controls are in place in some but not all cases		13%
Yes, and we are comfortable that suitable controls are in place in all cases		33%

Q6.8 Does your Fund have a specific data breach policy? (tick one)

Yes, we have a Fund specific data breach policy		21%
No, we do not have a Fund specific data breach policy as we follow the Host Authority's policy	Y	79%
No, we do not have a data breach policy that we follow		0%

**Your Response      Scorecard**

Q7.1 Which best describes your understanding of the asset flows in your Fund? (tick one)

- We have not yet considered where/how the assets flow
- We understand the main asset flows and have documented these but it is not comprehensive
- We have a comprehensive asset map which documents all of the asset movements, from contributions arriving to receipt of investment income and benefit payments.

	17%
	75%
<b>Y</b>	8%

Q7.2 Which of the following approaches are used when the senior officers authorise disinvestment instructions? (tick all that apply)

- Unencrypted email
- Email with encrypted attachment
- Other secure email or file sharing portals
- Physically signed and posted
- Other (please specify)

<b>Y</b>	50%
	29%
	38%
	50%
	17%

Additional comments

Q7.3 If a disinvestment took place from a manager, how long would it be before the Fund officers were notified that it had taken place (as different managers have different timescales, and arrangements in the new pooling arrangements may differ from non-pooled assets, please indicate what is typical)? (tick one)

- Within 24 hours
- Within 2 working days
- Within 5 working days
- Longer
- We are not notified
- Additional comments

<b>Y</b>	54%
	25%
	4%
	4%
	4%

Q7.4 How many individuals from the Fund/administering authority can authorise disinvestment of assets? (tick one)

- None
- 1
- 2 or 3
- 4 or 5
- Over 5

	0%
	4%
<b>Y</b>	54%
	17%
	21%

Q7.5 How many individuals can authorise payments from the Fund's bank account? (tick one)

- None
- 1
- 2 or 3
- 4 or 5
- Over 5

**Your  
Response      Scorecard**

	0%
	0%
Y	29%
	25%
	42%



**Your  
Response      Scorecard**

Q8.1 Which of the following approaches are used to communicate individual scheme member information/data between officers (or its providers) and scheme members? (tick all that apply)

Unencrypted email	Y	33%
Email with encrypted attachment		54%
Other secure email or file sharing portal (including a member self-service facility)	Y	88%
Hard copy information via post	Y	83%
Other (please specify)		8%

Q8.2 If you have a scheme member website/on-line facility, does it include the following? (tick all that apply)

Publication of generic Fund documents	Y	100%
Generic information for members	Y	100%
Access to individual data and quotes via personal log in	Y	96%
Ability to update individual record via personal log in	Y	92%
We do not have a scheme member website		0%
Other (please specify)		0%

Additional comments

Q8.3 Have you conducted a security assessment of your Fund's website? (tick one)

We have no Fund website

No assessment undertaken

External assessment but more than 24 months ago

External assessment within last 24 months

We rely on the provider to do checks on our behalf and we receive a report from time to time

We rely on the provider to do checks on our behalf but we don't get any reports on the findings or we don't know when the checks were last done

	0%
	0%
	0%
Y	33%
	17%
	46%

**Your Response      Scorecard**

Q8.4 Have you conducted a security assessment of your scheme member on-line access (where they access personal data)? (tick one)

- We have no scheme member on-line facility
- No assessment undertaken
- External assessment but more than 24 months ago
- External assessment within last 24 months
- We rely on the provider to do checks on our behalf and we receive a report from time to time
- We rely on the provider to do checks on our behalf but we don't get any reports on the findings or we don't know when the checks were last done

	4%
	0%
	4%
Y	29%
	25%
	38%

Q8.5 What security arrangements are in place for scheme members to access personal data via the Fund's website/on-line facility? (tick all that apply)

- Member passwords have minimum standards (e.g. combination of letters and numbers)
- Member passwords need to be changed periodically
- Two factor approval is required (e.g. email and text messages with details)
- Don't know
- Not applicable – we have no website/on-line facility with personal data
- Other (please specify)

Y	88%
Y	17%
	8%
	4%
	4%
	13%

Additional comments

Q8.6 What validation is done when a scheme member contacts the administration team? (tick one)

- Minimum personal data checks are required (e.g. confirmation of date of birth and address)
- Minimum personal and fund specific data checks are required (e.g. service dates or benefit category)
- We usually gather some information from them but we have no documented policy on this
- None

	67%
Y	21%
	4%
	0%

**Your  
Response      Scorecard**

Q8.7 What validation is done when benefits are paid to members or transferred to another pension scheme? (tick one)

Original or formally certified documents (such as birth and other name change certification)		29%
Certificates, as above, but we accept photocopies with no certification	Y	54%
Biometric checks		0%
Combination of the above		13%
Other (please specify)		0%

Additional comments

Q8.8 Are members warned of the risks of scams and cyber threats (tick one)

Yes, regularly (at least annual)		71%
Yes, from time to time	Y	21%
No		4%

Q8.9 Are pension fund members notified of how the Fund manages cyber risk and actions? (tick all that apply)

No	Y	71%
Yes we include an update in our annual communication (e.g. newsletter or annual benefit statement)		8%
Yes we include details in our Report and Accounts		0%
Yes we provide updates via our member website		17%
Other (please specify)		4%

Additional comments

**Your Response      Scorecard**

Q9.1 Do you have a cyber Incident Response Plan and/or any of the component parts (whether in a formal plan or stand-alone)? (tick all that apply)

Pension Fund cyber incident response plan		8%
Host Authority developed cyber incident response plan	Y	83%
Incident response decision tree		21%
Fund officer, provider, employer, Committee and Board contact details		46%
Assessment tools e.g. checklists, severity guidance		17%
Communication and media checklist		21%
Data Breach protocol (i.e. GDPR)		71%
None of the above		0%
Other (please specify)		4%

Additional comments

Q9.2 Has the Fund Incident Response Plan (or component parts) been seen and contributed to by the Host Authority? (tick one)

Yes, actively contributed and seen		21%
Not actively contributed but it has been shared with Host Authority		21%
Neither seen nor contributed		4%
We have no Fund specific plan	Y	50%

Q9.3 Has your response to an incident been tested with a "war game" simulated attack? (tick one)

No		58%
Yes at a basic level	Y	33%
Yes in detail, stepping through all parts of the plan		4%

**Your Response      Scorecard**

Q9.4 Do the Fund officers have access to specialist support in the event of a cyber attack? (tick all that apply)

No		0%
We have access to support from the Host Authority's cyber team	Y	88%
We have external cyber support on retainer that we can access which is provided via the Host Authority	Y	25%
We have external cyber support on retainer that we have commissioned directly for the Fund		0%
We have access via the Host Authority's insurance arrangements		29%
We have access via Fund specific insurance arrangements		0%
Don't know		13%
Other (please specify)		0%

Q9.5 In the event that you needed to contact members (actives and non-actives) urgently about a cyber breach, what proportion of members do you hold email addresses for? (tick one)

Under 30%		29%
30 - 50%	Y	46%
50 - 70%		17%
Over 70%		0%
Don't know		8%

**Your  
Response      Scorecard**

Q10.1 Have the Fund officers assessed the possible financial impact of a cyber attack on the Fund, Council, other employers or providers? (tick one)

- No
- Yes at a high level
- Yes in some detail, including the impact of different types of attack

<b>Y</b>	67%
	29%
	0%

Q10.2 Do you have any insurance policies in place which cover cyber attacks on the Fund? (tick all that apply)

- No
- We have cyber insurance as the Fund is covered as part of the Host Authority/Council's policy
- We have our own Fund cyber insurance policy
- Other insurance (please specify)

<b>Y</b>	54%
	38%
	0%
	4%

Q10.3 What work has been undertaken to review the cyber clauses in your provider contracts? (tick one)

- None
- Basic assessment of some cyber clauses
- Detailed assessment and understanding for some providers but not all
- Detailed assessment and understanding of the cyber clauses for all key providers

	33%
<b>Y</b>	46%
	13%
	8%

Final additional comments