PENSIONS AND LIFETIME SAVINGS ASSOCIATION

Aon LGPS Cyber Scorecard

Summary report for:
Isle of Wight Council Pension Fund

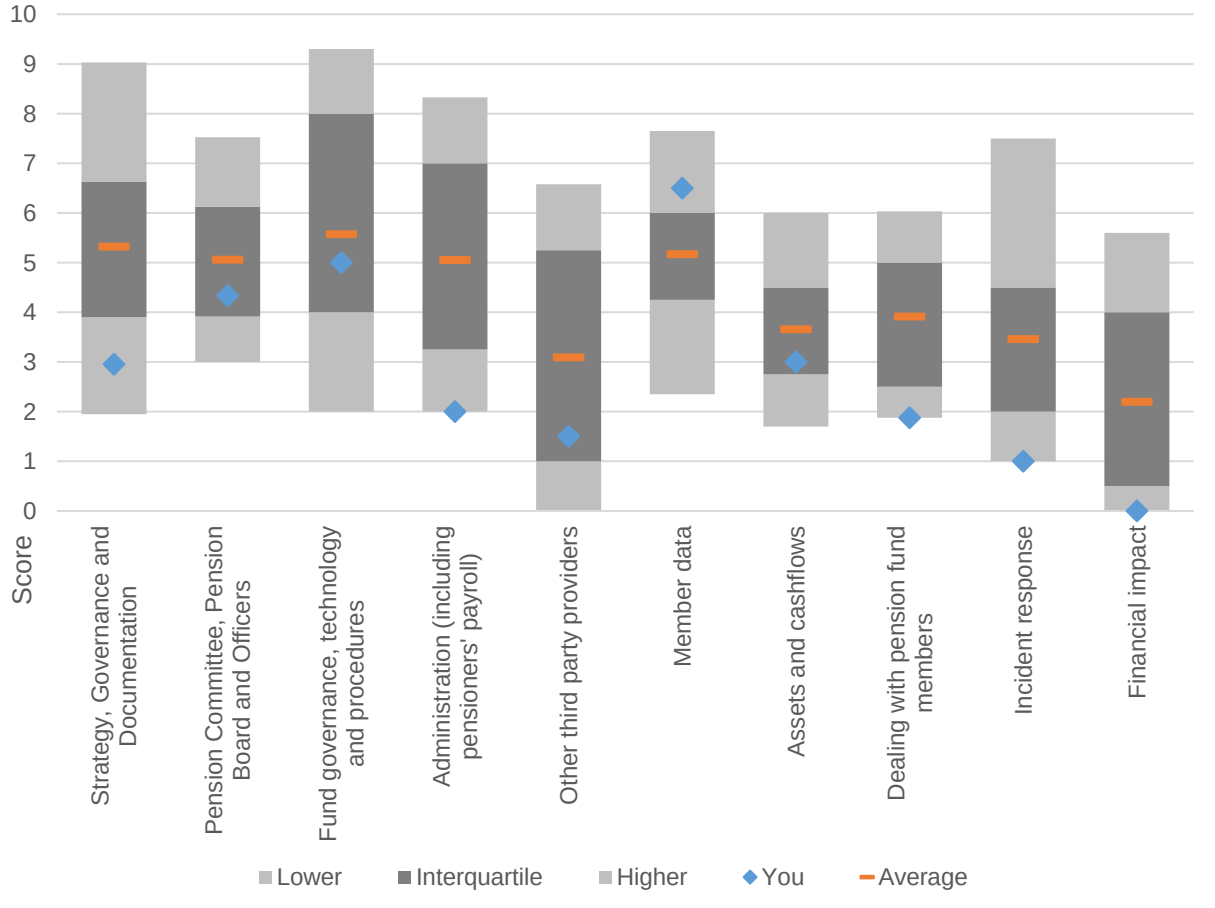
Based on responses by:
Jo Thistlewood

Date : 6 October 2022

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.



AON

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.

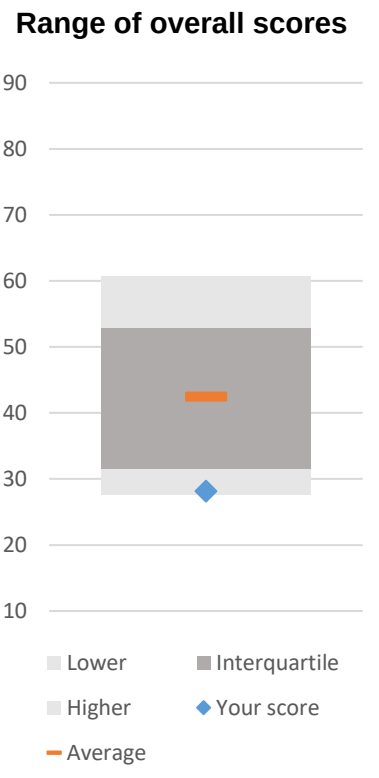
	Section scores (out of 10)		
	Your score	**Average**	
Strategy, Governance and Documentation	3.0	5.3	Lower
Pension Committee, Pension Board and Officers	4.3	5.1	Interquartile
Fund governance, technology and procedures	5.0	5.6	Interquartile
Administration (including pensioners' payroll)	2.0	5.1	Lower
Other third party providers	1.5	3.1	Interquartile
Member data	6.5	5.2	Upper
Assets and cashflows	3.0	3.7	Interquartile
Dealing with pension fund members	1.9	3.9	Lower
Incident response	1.0	3.5	Lower
Financial impact	0.0	2.2	Lower
Overall score	28.2	42.5	

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.



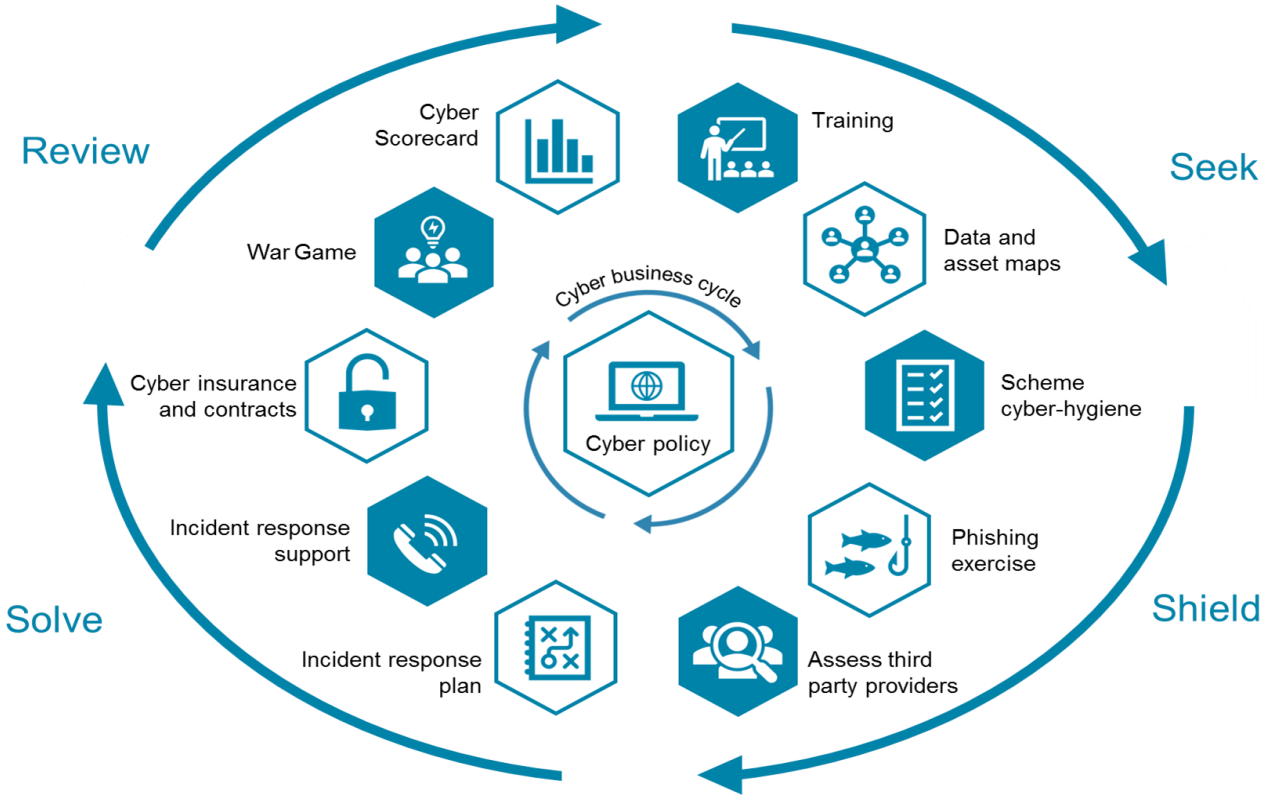
Contacts

Chris Emmerson
Consultant
+44 (0)117 945 3521
chris.emmerson@aon.com

Jason Wilson
Senior Consultant
+44 (0)207 086 4257
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 PLSA

The Pensions and Lifetime Savings Association is the voice of workplace pensions and savings. We represent pension schemes that together provide a retirement income to more than 30 million savers in the UK and invest more than £1.3 trillion in the UK and abroad. Our members also include asset managers, consultants, law firms, fintechs, and others who play an influential role in people's financial futures. We aim to help everyone achieve a better income in retirement.

Registered office : 6th Floor, 24 Chiswell Street, London, EC1Y 4TY
www.plsa.co,uk

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.

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

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		6%
We are currently in the process of assessing our fund cyber risks	Y	51%
We have assessed the specific cyber risks that our fund is exposed to		54%
In assessing those risks we have consulted the Host Authority (Council)		74%
In assessing those risks we have consulted our key advisers and providers		46%
In assessing those risks we have consulted a cyber specialist		17%
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	Y	37%
We rely on our Host Authority's cyber strategy	Y	74%
We have a Fund cyber policy document that captures our cyber strategy		20%
Our Fund cyber policy document has been reviewed in the past 24 months		23%
Our Fund cyber policy document has been developed in conjunction with the Council		23%
We had specialist cyber support when preparing our Fund's cyber policy document		6%
Q1.3 For your Fund who has primary responsibility for cyber risk? (tick one)		
Chair of Committee		0%
All Committee members collectively		6%
Chief Finance Officer (i.e. Section 151 Officer in England)		29%
The Senior Pension Fund Officer (who is not the S151 Officer)	Y	23%
Dedicated Cyber Officer or IT Officer from the Host Authority		17%
Providers		0%
We have not yet allocated primary responsibility		17%
Other – please specify		9%

	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		37%
Yes – usually at least once a year		29%
Yes – but generally less than once a year		14%
No	Y	20%
Q1.5 Does the Pension Board receive updates on cyber risks, controls and incidents affecting the Fund?		
Yes – at every meeting	Y	40%
Yes – usually at least once a year		29%
Yes – but generally less than once a year		11%
No		20%
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		3%
Cyber risks are included in our risks register	Y	97%
The cyber risks in our risk register are reviewed at least once every 12 months		74%
We have reconsidered the information relating to our cyber risk on the risk register during 2020 due to the Covid-19 pandemic		51%

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)	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		94%	80%	34%
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	89%	80%	60%
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		100%	80%	29%
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			91%	46%	20%
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				54%	26%	17%

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

	Your Response			Scorecard		
	Officers	PC Members	PB Members	Officers	PC Members	PB Members
Our training program includes training on cyber risk at least annually				63%	43%	43%
Our training program includes training on cyber risk but less frequently than annually	Y			17%	20%	17%
Our training program does not include training on cyber risk				0%	9%	9%
Our training includes specialist cyber resources as well as pension experts				29%	20%	17%
Our training on cyber risk is provided purely as part of the Host Authority's training	Y	Y	Y	51%	40%	23%

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

	Your Response	Scorecard
Our Committee/Board members and officers have no specific training on phishing risks		9%
Some but not all of our Committee/Board members and officers are trained on phishing risk	Y	60%
All of our Committee/Board members and officers are trained on phishing risks, including simulated phishing attacks		14%
I don't know		17%

	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	Y	46%
Email with encrypted attachment	Y	26%
Other secure email facility or file sharing portal		29%
Committee/Board portal (e.g. online meeting packs or Host Authority Committee portal)	Y	80%
Hard copy information via post	Y	46%
Other - Please specify		9%
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		17%
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	20%
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		63%
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	66%
Yes, our password is unlikely to have changed in that time		6%
Yes, although our password changes it follows the same structure (eg ABC2019! becomes ABC2020!)		3%
No, our password(s) change regularly and do not have a pattern		23%

	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		9%
In house	Y	86%
Shared Services		6%
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		6%
Request provider's own standard cyber policy documents	Y	71%
Fund-specific questionnaire		14%
Host Authority's cyber questionnaire for providers		40%
Interview with provider		20%
Site visit		3%
Other (please specify)		20%
Q4.3 How regularly do you assess the administration provider and platform? (tick one)		
Never		6%
At least annually		54%
At least every 2 years		3%
Ad-hoc, no formal policy	Y	26%
Other (please specify)		11%
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		63%
Details of network security and penetration testing		80%
Detail of staff training and user access		49%
Controls around transfer of data		43%
Physical security provisions		31%
Incident response planning		63%
Other (please specify)		17%

	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		49%
No	Y	49%
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	Y	69%
No, but the pensioners' payroll is subject to a cyber assessment at least annually		9%
No, but the pensioners' payroll is subject to a cyber assessment at least every 2 years		0%
No, but the pensioners' payroll is subject to a cyber assessment on an ad-hoc basis (no formal policy)		11%
No and the pensioners' payroll has not been subject to a cyber assessment		3%
No and I do not know if the pensioners' payroll has been subject to a cyber assessment		6%
Other (please specify)		3%

	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		34%
Benefits Consultant		9%
Governance Consultant		6%
Investment Consultant		17%
Investment Managers		23%
Pooling Operator		20%
Custodian		26%
Lawyers		0%
External Auditors		9%
AVC providers		11%
Communications advisors		0%
Host Authority (e.g. Council)	Y	54%
Other employers		0%
Tracing Service provider		14%
		20%

Additional comments

we have not carried out any formal assessments on any of our providers

	Your Response	Scorecard
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	Y	37%
Request provider's own standard cyber policy documents		54%
Fund-specific questionnaire		14%
Council's cyber questionnaire for suppliers		23%
Interview with provider		11%
Site visit		0%
Other (please specify)		6%

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		31%
At least annually		23%
At least every 2 years		9%
Ad-hoc, no formal policy	Y	26%
Other (please specify)		11%

Additional comments

will generally review cyber issues at procurement stage if seeking new provider

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		49%
Details of network security and penetration testing		51%
Detail of staff training and user access		29%
Controls around transfer of data		40%
Physical security provisions		26%
Incident response planning		37%
Other (please specify)		17%

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		34%
No	Y	57%

	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		20%
We understand the main data flows and have documented these but it is not comprehensive	Y	66%
We have a comprehensive data map which documents all of the places that our member data is used and transferred		11%
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		20%
Email with encrypted attachment		69%
Other secure email or file sharing portal	Y	89%
Hard copy information via post (e.g. leaver forms)		46%
Other (please specify)	Y	14%
i-connect		
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		3%
Email with encrypted attachment		60%
Other secure email		51%
File sharing portal e.g. secure employer data upload site		74%
Other (please specify)	Y	20%
i-connect		
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		23%
No assessment undertaken		3%
External assessment but more than 24 months ago		0%
External assessment within last 24 months		26%
We rely on the provider to do checks on our behalf and we receive a report from time to time	Y	23%
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		23%

	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		6%
Email with encrypted attachment	Y	86%
Other secure email or file sharing portal	Y	80%
Hard copy information via post (e.g. leaver forms)		54%
Other (please specify)	Y	9%
usually other party's portal		
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		9%
Email with encrypted attachment		49%
Other secure email or file sharing portal	Y	94%
Other (please specify)		9%
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		40%
We don't know	Y	9%
Yes, but we don't have any insight into the controls		11%
Yes, and we are comfortable that suitable controls are in place in some but not all cases		14%
Yes, and we are comfortable that suitable controls are in place in all cases		26%
Q6.8 Does your Fund have a specific data breach policy? (tick one)		
Yes, we have a Fund specific data breach policy		34%
No, we do not have a Fund specific data breach policy as we follow the Host Authority's policy	Y	66%
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		9%
We understand the main asset flows and have documented these but it is not comprehensive	Y	63%
We have a comprehensive asset map which documents all of the asset movements, from contributions arriving to receipt of investment income and benefit payments.		20%

Q7.2 Which of the following approaches are used when the senior officers authorise disinvestment instructions? (tick all that apply)		
Unencrypted email		46%
Email with encrypted attachment	Y	29%
Other secure email or file sharing portals	Y	51%
Physically signed and posted	Y	46%
Other (please specify)		31%

Additional comments

depends on the investment manager and their required protocols

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		54%
Within 2 working days	Y	20%
Within 5 working days		6%
Longer		3%
We are not notified		9%

Additional comments

Q7.4 How many individuals from the Fund/administering authority can authorise disinvestment of assets? (tick one)		
None		3%
1		6%
2 or 3	Y	40%
4 or 5		20%
Over 5		23%

	Your Response	Scorecard
Q7.5 How many individuals can authorise payments from the Fund's bank account? (tick one)		
None		0%
1		0%
2 or 3		20%
4 or 5		26%
Over 5	Y	46%

	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		37%
Email with encrypted attachment		57%
Other secure email or file sharing portal (including a member self-service facility)	Y	83%
Hard copy information via post	Y	83%
Other (please specify)		11%

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	97%
Generic information for members	Y	100%
Access to individual data and quotes via personal log in	Y	94%
Ability to update individual record via personal log in	Y	94%
We do not have a scheme member website		0%
Other (please specify)		0%

Additional comments

pension fund website holds generic scheme and local information and copy forms. Member self service portal holds

Q8.3 Have you conducted a security assessment of your Fund's website? (tick one)		
We have no Fund website		3%
No assessment undertaken		6%
External assessment but more than 24 months ago		0%
External assessment within last 24 months		29%
We rely on the provider to do checks on our behalf and we receive a report from time to time		20%
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	Y	37%

	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		6%
No assessment undertaken		0%
External assessment but more than 24 months ago		0%
External assessment within last 24 months		40%
We rely on the provider to do checks on our behalf and we receive a report from time to time	Y	23%
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		29%

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)		89%
Member passwords need to be changed periodically		29%
Two factor approval is required (e.g. email and text messages with details)		17%
Don't know		3%
Not applicable – we have no website/on-line facility with personal data		6%
Other (please specify)	Y	23%

member specific password, but no minimum standard

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)	Y	77%
Minimum personal and fund specific data checks are required (e.g. service dates or benefit category)		14%
We usually gather some information from them but we have no documented policy on this		3%
None		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)		31%
Certificates, as above, but we accept photocopies with no certification	Y	63%
Biometric checks		0%
Combination of the above		6%
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)	Y	66%
Yes, from time to time		31%
No		3%
Q8.9 Are pension fund members notified of how the Fund manages cyber risk and actions? (tick all that apply)		
No	Y	69%
Yes we include an update in our annual communication (e.g. newsletter or annual benefit statement)		11%
Yes we include details in our Report and Accounts		6%
Yes we provide updates via our member website		20%
Other (please specify)		11%
Additional comments		
scams warning are included in every transfer letter and within annual newsletters to members.		

	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		14%
Host Authority developed cyber incident response plan	Y	77%
Incident response decision tree		26%
Fund officer, provider, employer, Committee and Board contact details		57%
Assessment tools e.g. checklists, severity guidance		20%
Communication and media checklist		11%
Data Breach protocol (i.e. GDPR)		69%
None of the above		3%
Other (please specify)		9%

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		26%
Not actively contributed but it has been shared with Host Authority		11%
Neither seen nor contributed		9%
We have no Fund specific plan	Y	51%

Q9.3 Has your response to an incident been tested with a "war game" simulated attack? (tick one)		
No	Y	63%
Yes at a basic level		29%
Yes in detail, stepping through all parts of the plan		3%

	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	Y	3%
We have access to support from the Host Authority's cyber team		83%
We have external cyber support on retainer that we can access which is provided via the Host Authority		23%
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		17%
We have access via Fund specific insurance arrangements		3%
Don't know		11%
Other (please specify)		6%

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%		17%
30 - 50%		51%
50 - 70%	Y	14%
Over 70%		0%
Don't know		14%

	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	Y	69%
Yes at a high level		29%
Yes in some detail, including the impact of different types of attack		0%
Q10.2 Do you have any insurance policies in place which cover cyber attacks on the Fund? (tick all that apply)		
No	Y	63%
We have cyber insurance as the Fund is covered as part of the Host Authority/Council's policy		29%
We have our own Fund cyber insurance policy		0%
Other insurance (please specify)	Y	20%
Council does not currently have cyber insuirance		
Q10.3 What work has been undertaken to review the cyber clauses in your provider contracts? (tick one)		
None		26%
Basic assessment of some cyber clauses		49%
Detailed assessment and understanding for some providers but not all		11%
Detailed assessment and understanding of the cyber clauses for all key providers		6%
Final additional comments		
Q1.5: board receive report at every meeting if an incident has been reported, not necessarily as a standing item.		