Audit West

Internal Audit Report
Confidential

Avon Pension Fund

Cyber Security - User Education and Awareness

September 2023

Executive Summary

Audit Opinion:

Assurance Rating	Opinion
Level 5 - Full Assurance	The systems of internal control are excellent with a number of strengths, no weaknesses have been identified and full assurance can be provided over all the areas detailed in the Assurance Summary.
Level 4 - Substantial Assurance	The systems of internal control are good with a number of strengths evident and substantial assurance can be provided as detailed within the Assurance Summary.
Level 3 - Reasonable Assurance	**The systems of internal control are satisfactory and reasonable assurance can be provided. However, there are a number of areas detailed in the Assurance Summary which require improvement and specific recommendations are detailed in the Action Plan.**
Level 2 - Limited Assurance	The systems of internal control are weak and only limited assurance can be provided over the areas detailed in the Assurance Summary. Prompt action is necessary to improve the current situation and reduce the levels of risk exposure.
Level 1 - No Assurance	The systems of internal control are poor, no assurance can be provided and there are fundamental weaknesses in the areas detailed in the Assurance Summary. Urgent action is necessary to reduce the high levels of risk exposure.

Assurance Summary:

Assessment	Risks
Satisfactory	User awareness and understanding of cyber risks and security procedures are not enhanced or maintained at acceptable levels.
Satisfactory	Users see cyber security policies and procedures as conflicting with delivering their primary job role or function.

Detailed Report

Opinion

Internal Audit has undertaken a review of the risks and controls related to the Avon Pension Fund's (APF) cyber security user education and awareness processes. We have assessed the framework of internal control at Level 3, reasonable assurance.

Scope and Objectives

The scope and objectives of our audit were set out in the Audit Brief and a summary of our opinion against each of the specific areas reviewed has been detailed in the Assurance Summary section above.

Context

The Pensions Regulator (PR) requires workplace pension trustees and scheme managers to protect pension scheme members and assets from cyber security threats. To help pension schemes build cyber resilience, the PR has published "Cyber security principles". One of these principles is that "all staff, and trustees, should receive training appropriate to their role at an appropriate frequency". The PR also references guidance from the National Cyber Security Centre (NCSC) including "10 Steps to Cyber Security". User engagement and training is the second of the 10 steps.

Cyber (or information) security training aims to give people the skills and knowledge they need to work securely. Training not only helps protect the organisation, but also demonstrates that staff are valued, and recognises their importance to the organisation.

This audit evaluated APF's security training and awareness raising arrangements against the criteria described in the national and pensions sector guidance:

- National Cyber Security Centre's (NCSC) "10 Steps to Cyber Security"
- Information Commissioner's Office (ICO) "Accountability Framework" and "A practical guide to IT security"
- Pensions Regulator's (PR) "Cyber security principles for pension schemes"
- ISO/IEC 27001 Information Security Management.

The Avon Pension Fund (APF) workforce is employed by Bath & North East Somerset Council (B&NES). Accordingly, the B&NES cyber security e-learning and policy frameworks for information security and data protection apply to APF.

We have therefore reported our findings and made recommendations to the Information Governance Manager and IT Service Delivery Manager, for B&NES, and they have agreed to implement all our recommendations by the end of the 2023-24 financial year. We will update APF on progress in implementing these recommendations once we have completed a follow up review as part of our 2024-25 audit plan.

Audit Comment

Our "Reasonable" assurance opinion is based on the evidence provided by the APF Governance Team and a review of the B&NES training course content and policies. We have considered the strengths and weaknesses in forming our opinion (see Appendix A).

The APF Governance team oversee both cyber security and data protection training for APF. Their approach takes steps beyond those provided by the B&NES cyber security and data protection training programmes. For example, APF track training delivery, arrange further training, and have an ongoing awareness raising email campaign. These additional measures offset some weaknesses in the B&NES training and awareness raising programme. Training and

awareness raising for handling personal data are notably stronger than those for cyber security topics.

Appendix A sets out our assessment of the level of compliance with the guidance in 10 Steps. We have briefly described the strengths and weaknesses that support the assessment and summarised the action we have agreed with the Information Governance Manager. Items marked "PR" are from the Pensions Regulator's Cyber security principles.

Audit & Risk Personnel

Lead Auditor: Tariq Rahman and Neil Roper

Acknowledgements:

Sincere thanks to Geoff Cleak, Liz Woodyard, Carolyn Morgan, Charlotte Curtis and all service staff for all their help and assistance throughout the Audit Review.

Appendix A – Compliance with NCSC and Pensions Regulator guidance

1. LEAD BY EXAMPLE					
	Requirement	**APF Compliance**	**Compliance strengths**	**Non-compliance weakness**	**Action agreed with Information Governance**
1.1	Senior leaders follow security policies and procedures e.g., use standard equipment, attend training etc.	Substantial	The Pensions and Investment managers use standard equipment and attended most of the recent cyber security and data protection training.		
1.2	Involve senior leadership in cyber security awareness campaigns.	Partial	Four security related articles have been published in the B&NES "Staff Briefing" newsletter.	B&NES senior leaders are not involved in promoting cyber security e-learning and awareness to the workforce. If senior leadership are not seen to be promoting and following cyber security messages, then this will undermine their effectiveness.	The Cyber Security Operational Group (CySOG) will ask the CEO and COO to promote the new cyber security training following the launch of the new MHR Ltd. Learning Management System.

2. EFFECTIVE SECURITY DIALOGUE WITH USERS					
	Requirement	**APF Compliance**	**Compliance strengths**	**Non-compliance weakness**	**Action agreed with Information Governance**
2.1	Understand what may prevent users from following security procedures and practices.	Partial	APF track data breach incidents, implement containment and improvement actions, and look for process improvements.	There is no user engagement process to find barriers that hinder users in following security procedures and practices. Users see established security procedures and practices as hindering their work.	Users will be invited to give feedback on security policies and processes via the cyber security messages intranet page.

2. EFFECTIVE SECURITY DIALOGUE WITH USERS					
	Requirement	**APF Compliance**	**Compliance strengths**	**Non-compliance weakness**	**Action agreed with Information Governance**
2.2	Security policies are fit for purpose and proportionate: - Include people with knowledge of local working environments in security policy making. - Provide routes to challenge security processes that do not work well in practice.	Substantial	The information security policy reflects best practice and is comparable to those used by other local authorities.	There is no mechanism to invite and capture feedback from users and teams about security processes and procedures that do not work well in practice. Users see established security procedures and practices as hindering their work.	As above.
PR	Implement a range of policies and processes around: - acceptable use of devices, email and internet - passwords and other authentication - home and mobile working - data access, protection (including encryption), use and transmission	Partial	The security policies are published on the intranet. The password policy is Appendix A to the Information Security Policy. APF delivered data protection and security training for working from home during the COVID pandemic response.	Key policies have not been updated recently: - Information security IGTEM 002-20 (2020) - Data breach management IGTEM 005-20 (2020) - Information sharing policy and guidelines (2018) - Mobile and remote working policy (2014). More recent homeworking guidance (from 2021 and 2022) on the intranet also refers to superseded Skype and Citrix technologies. Outdated policies may be seen as no longer relevant or give the impression that the organisation is not serious about cyber security. The mobile and remote working policy is not included in the "Policy" section of the Information Governance policies and guidelines intranet page.	CySOG will include the Information Security Policy in their schedule of policy reviews. Information Governance will schedule reviews of the Information Governance and data breach policies.

2. EFFECTIVE SECURITY DIALOGUE WITH USERS					
	Requirement	**APF Compliance**	**Compliance strengths**	**Non-compliance weakness**	**Action agreed with Information Governance**
				Users may overlook the remote working policy and hence be unaware of the Councils approach to minimising information risks when working outside the office environment.	
2.3	Encourage people to report cyber security issues and incidents: - establish reporting processes - publish and promote the reporting processes	Substantial	Cyber incident reporting uses the personal data breach reporting process (IGTEM 005-20). Suspicious and malicious email reporting is described on the "Cyber Security Messages" intranet page. APF have extended the incident reporting process to create their own record and capture regulatory breaches.	IGTEM 005-20 is personal data specific and does not cover reporting phishing or malware attacks. Users do not know how to respond to, or "call out", potential cyber threats they experience. IT Services are not routinely notified of incidents reported under IGTEM 005-20 data breach reporting process. IT Services may not be able to respond promptly to incidents reported via the data breach incident reporting form.	CySOG are developing a cyber security incident management policy and process, and this will be linked to the training materials in the new Learning Management System. As above.
2.4	Regard security incidents as an opportunity for improvement for both the individuals involved and the organisation.	Substantial	APF review data and regulatory breach incidents to identify additional training needs and opportunities for process improvement.		

3. SECURITY AWARENESS CAMPAIGNS					
	Requirement	**APF Compliance**	**Compliance strengths**	**Non-compliance weakness**	**Action agreed with Information Governance**
3.1	Analyse the impact of security awareness raising campaigns and measures over time. Security awareness campaigns are unlikely to deliver immediate results, so it is important to measure effectiveness only over the medium and long term.	None		User cyber security awareness levels are not measured. APF track incidents and breaches, but it is not clear how these are used to monitor trends over time or how they are mapped against awareness raising campaigns e.g., the Friday bite size reminders. The level of cyber security awareness in the workforce is not known and APF cannot measure how effective any awareness campaigns are.	The new Learning Management System will supply information on course completion rates and achievement levels. Additional awareness raising techniques (see below) will be introduced and this will also facilitate some measurement of cyber security awareness levels in the Council.
3.2	Make cyber security messages relevant to the workforce and organisation.	Substantial	Friday bitesize data protection reminders are used to provide messages relevant to the pensions team.	The personal information and 'sensitive' personal information examples given in the bitesize reminders may not reflect the data processed in the Altair pensions administration system. Security messages that do not use information and terminology relevant to the workforce may not have the desired results. In some cases, they may have a negative impact as it shows a lack of appreciation of the workflows and data processed.	
3.3	Make cyber security messages positive. Focus on what people can do to help rather the consequence of them doing something they shouldn't.	Full	The Friday bitesize reminders gave positive security messages.		

3. SECURITY AWARENESS CAMPAIGNS					
	Requirement	**APF Compliance**	**Compliance strengths**	**Non-compliance weakness**	**Action agreed with Information Governance**
3.4	Use a range of approaches to build user engagement in cyber security.	Partial	Friday bite size briefing include polls and approximately 30% respond.	Other security activities are not used beyond the awareness raising briefings and training. Making people aware of security risks and what to do about them, does not necessarily mean that they will (or are able to) adopt those behaviours.	CySOG will be introducing other awareness raising techniques (e.g., simulations, and workshops) to engage with users.

4. CYBER SECURITY TRAINING					
	Requirement	**APF Compliance**	**Compliance strengths**	**Non-compliance weakness**	**Action agreed with Information Governance**
4.1	Develop cyber security training to deliver the knowledge and behaviours that users need.	Substantial	Training is delivered via e-learning: - currently, the NCSC "Stay Safe Online". - before this a bespoke training module developed for B&NES by Cylix. "Stay Safe Online" addresses what the NCSC consider to be the most important cyber security knowledge and behaviours for people in the UK.	The "Stay Safe Online" password guidance is not fully consistent with that in the B&NES Information Security Policy Appendix A and "Password for life" intranet page. Differences can be seen in the treatment of: - password length - password complexity - storing passwords in browsers and password managers Differences between the policy, published guidance, and cyber security e-learning may undermine user confidence and the training may become ineffective.	CySOG have created a new password policy, and this will be linked to the training materials in the Learning Management System.

4. CYBER SECURITY TRAINING					
	Requirement	**APF Compliance**	**Compliance strengths**	**Non-compliance weakness**	**Action agreed with Information Governance**
PR	All staff, and trustees, receive training appropriate to their role.	Substantial	APF monitor completion of cyber security and data protection training. All APF users completed the Cylix cyber security e-learning.		
PR	The training should include awareness of cyber risks and how to report incidents.	Partial	"Stay Safe Online" addresses key cyber risk areas and has a lesson on incident reporting.	"Stay Safe Online" does not include a link to the Council's incident reporting process.	CySOG are developing a cyber security incident management policy and process, and this will be linked to the training materials in the new Learning Management System.
4.2	Highlight the benefits of cyber security training to users.	None	Some benefits are implied in the "Stay Safe Online" introduction video.	The benefits of cyber security training are described on the Learning Pool cyber security page or in the "Stay Safe Online" lessons. Users do not feel personally invested in cyber security and are less likely to adopt good security behaviours.	The benefits of cyber security training will be included in the new Learning Management System content.
4.3	Deliver cyber security training in small, frequent chunks.	Partial	"Stay Safe Online" is a short, easily digested course.	"Stay Safe Online" is a single module, designed to be delivered in a single session and does not facilitate "small frequent chunks" delivery. Cyber security training is forgotten and rates of threat recognition decline. Research into recognition of malicious email found training improved response rates for only six months.	Periodic refresher training for cyber security will be included in the new Learning Management System training programme.

4. CYBER SECURITY TRAINING					
	Requirement	**APF Compliance**	**Compliance strengths**	**Non-compliance weakness**	**Action agreed with Information Governance**
PR	All staff, and trustees, receive training at an appropriate frequency. The ICO also expects staff complete refresher training at appropriate intervals.	Partial	APF staff must refresh their cyber security and data protection training every 3 years. This is tracked using the training completion spreadsheet.	Three years refresh frequency is too long for cyber security training. Cyber security training is forgotten and rates of threat recognition decline (see above). Cyber threats evolve rapidly and training from three years ago may not help users in identifying current attacks.	As above.
4.4	Revise cyber security training regularly to keep it fresh.	Partial	Cyber security e-learning was updated to "Stay Safe Online" in 2022. APF users will therefore see training content different from that at their previous training.	There is no process to regularly update the cyber training content. "Stay Safe Online" was the first update since 2018. Users may see repetitious and stale training as a sign that the organisation sees it as unimportant.	CySOG aim to update the cyber security e-learning more often however there is no timetable for future updates.
4.5	Use trainers who have sufficient knowledge of the subject and who can relate it to the trainee's everyday work.	Not applicable	Training uses e-learning modules rather than face to face training.		