Cyber security for Pension Schemes

Pension Schemes should review their approach to cyber risk to comply with the General Code of Practice

Trustees and Scheme Managers need to understand how their pension scheme providers and administrators are protecting themselves, their funds and their members. Cyber attacks are increasing in volume and sophistication, meaning continual vigilance is crucial. The Pensions Regulator ('TPR') has recently introduced its General Code of Practice ('the Code'). All pension schemes with more than 100 members that are required to establish and operate an Effective System of Governance ('ESOG') should undertake and evidence an Own Risk Assessment ('ORA'). The ORA is an assessment of how well the ESOG is working and how risks, including cyber risks, are managed.

- Pension schemes hold large amounts of personal data which can make them an attractive target for fraudsters and criminals. As Trustees and Scheme Managers, you need to take steps to protect your members and assets accordingly, including protecting them against cyber risk.
- Worst case outcomes from a cyber attack include catastrophic loss of data, theft of scheme assets or fraudulent benefit claims.
- A major incident could do the same reputational damage to the sponsoring employer as a cyber risk failure in their main business.
- TPR has issued guidance to Trustees on what they need to do to mitigate their cyber risk exposure. They have also issued a General Code of Practice ("The Code") which outlines a number of cyber controls.

The Pensions Regulator recommends that 'you may want or need to have the effectiveness of your cyber risk management independently assessed (e.g. by an auditor) or seek specialised accreditation, such as ISO 27001.'

General Code of Practice

The Code sets out expectations that cyber risk is **assessed**:

- The governing body has knowledge and understanding of cyber risk.
- Cyber risk is recorded on the risk register and reviewed regularly.
- Vulnerability to a cyber incident is regularly assessed.
- Roles and responsibilities for cyber risk and cyber incidents are clearly defined and documented.

Cyber risk is **managed:**

- Systems are up to date with the latest security releases from vendors and preventative measures such as anti-virus/anti-malware solutions.
- Critical systems are regularly backed up.
- Policies for acceptable use of systems and devices are documented and enforced.
- Policies and procedures to assess reporting requirements for cyber breaches (e.g. to the Information Commissioner) are maintained.
- A cyber incident response plan is documented and regularly exercised.
- Schemes review their service providers' controls.
- Cyber security controls and procedures are in place and functioning.
- Once an ESOG is established and an initial ORA undertaken, each element, including cyber security measures should be reviewed at least every three years (or sooner if there is significant change to the scheme's governance or key risks).

We have a long heritage in the Pensions Industry supporting pension schemes in improving their cyber security posture. We have over 200 cyber security professionals in the UK and over 6,000 globally. Our cyber security specialists hold professional credentials such as CISSP, CISM, CISA and ISO 27001 Lead Auditors.

How we can support you in managing your cyber risk

Service	Key Question	Outcome and Benefits
Control Assessments	How mature are your cyber controls?	Our team of experienced cyber professionals can independently review and assess your cyber controls to provide practical actionable recommendations to improve your cyber security posture. We can also help you prepare for ISO/IEC 27001 (Information Security Management Systems) certification.
Cyber Boardroom Training	Is the Board cyber-aware?	We provide a range of cyber training and awareness services for Trustees, Pensions Committees, Senior Executives, Board and Non-Executives. This can include awareness sessions on current cyber threats, training to respond to cyber incidents to keep your Board/Trustees/Committee members/NEDs knowledgeable and appraised of the latest developments in cybersecurity.
Third Party Security	How do you know that your key suppliers are secure?	We can help you identify your highest risk suppliers, such as third party administrators, and conduct security reviews of those suppliers on your behalf. We have extensive experience in delivering Third Party Security, and our team conducts hundreds of reviews annually on behalf of our clients.
Incident Response	Is your organisation ready to respond to and recover from cyber attacks?	We can provide 24/7 Incident Response services on a retainer basis. Our incident response retainer offering is one of the most comprehensive in the industry. You will have access to highly trained staff and KPMG's suite of tools used for incident response and digital forensics.
Penetration Testing	Are IT systems and business processes suitably resistant to cyber attacks?	We can provide a security assessment of your IT systems and processes against specific cyber risks, in which we will demonstrate end-to-end attacks in practice. Upon completion of fieldwork, we will provide our consolidated analysis and improvement recommendations.
Privacy	Are you fulfilling your regulatory obligations for privacy?	Our Privacy Advisory Services provide you with risk-based solutions to meet your obligations, assess privacy controls and contextualise your risk appetite.
Threat Intelligence	What are the key emerging threats facing your organisation?	We can produce a quarterly, semi-annual or annual threat intelligence report on what is happening across the industry and examples of recent attacks. The report is designed for a range of audiences, it serves as a way to understand who the threat actors are and the types of cyber-attacks and should be a standard item for discussion at Board/Trustee/Pensions Committee meetings.

Contact us

Neil Coutts CISM, CRISC
Director,
Cyber and Technology Risk
T: +44 (0)7810 545 676
E: neil.coutts@kpmg.co.uk

Urrffa Rafiq BA Hons
Director,
Employer Reward Services
T: +44 (0)7714 140 643
E: urrffa.rafiq@kpmg.co.uk

kpmg.com/uk

Create: CRT156077A | May 2024