Cyber controls (ADM016)

'Cyber risk' refers to the risk of loss, disruption or damage to a scheme or its members as a result of the failure of its information technology systems and processes(see also **Identifying and assessing risks**). Governing bodies should take steps to reduce the risk of incidents occurring, and appropriately manage any incidents that arise. Properly functioning cyber controls will assist governing bodies in complying with data protection legislation,[CY1] and may reduce liabilities in the event of a data breach.

Under section 249A of the Pensions Act 2004,[CY2] governing bodies of certain schemes must establish and operate an effective system of governance (see **Scheme governance**) including internal controls (see **Managing risk using internal controls**). However, there are certain exemptions.[CY3] These controls need to include measures to reduce cyber risk.

Under section 249B of the Pensions Act 2004,[CY4] scheme managers of public service pension schemes are required to establish and operate internal controls, which are adequate for the purpose of securing that the scheme is administered and managed in accordance with the scheme rules,[CY5] and with the requirements of the law.[CY6]

The legal obligation to establish measures to reduce cyber risk is different for public service pension schemes.[CY7] As far as cyber controls is a matter set out in the scheme rules[CY8] or in the requirements of the law,[CY9] scheme managers of public service pension schemes must establish and operate adequate internal controls in relation to them. In such cases, internal controls need to include measures to reduce cyber risk.

To the extent that cyber risk does not fall (wholly or partly) within the last paragraph, it is good practice for scheme managers of public service pension schemes to adopt the measures set out below. Our expectations for the governing body's processes and procedures are summarised below. Governing bodies should also be aware of their responsibilities under the UK GDPR.

CY1 For example, Data Protection Act 2018 and the Retained Regulation (EU) 2016/679) (UK General Data Protection Regulation)
CY2 Articles 226A of The Pensions (Northern Ireland) Order 2005
CY3 Section 249A(3) Pensions Act 2004 [Article 226A (3) of The Pensions (Northern Ireland) Order 2005]
CY4 Articles 226B of The Pensions (Northern Ireland) Order 2005
CY5 As defined in section 318(1) of the Pensions Act 2004 [Article 2(2) of The Pensions (Northern Ireland) Order 2005]
CY6 As defined in Section 318(2) Pensions Act 2004 2004 [Article 2(3) of The Pensions (Northern Ireland) Order 2005]
CY7 As defined in section 318(1) of the Pensions Act 2004 [Article 2(2) of The Pensions (Northern Ireland) Order 2005]
CY8 As defined in Section 318(2) Pensions Act 2004 2004 [Article 2(3) of The Pensions (Northern Ireland) Order 2005]
CY9 The law includes the Data Protection Act 2018 and the Retained Regulation (EU) 2016/679) (UK General Data Protection Regulation)

Assessing cyber risk

- Ensure the governing body has knowledge and understanding of cyber risk.
- Understand the need for confidentiality, integrity and availability of the systems and services for processing personal data, and the personal data processed within them.
- Have clearly defined roles and responsibilities to identify cyber risks and breaches, and to respond to cyber incidents.
- Ensure cyber risk is on the risk register and regularly reviewed (see also **Managing risk using internal controls**).
- Assess, at appropriate intervals, the vulnerability to a cyber incident of the scheme's key functions, systems and assets (including data assets) and the vulnerability of service providers involved in the running of the scheme.
- Consider accessing specialist skills and expertise to understand and manage the risk.
- Ensure appropriate system controls are in place and are up to date (eg firewalls, anti-virus and anti-malware products).

Managing cyber risk

- Ensure critical systems and data are regularly backed up.
- Have policies for the use of devices, and for home and mobile working.
- Have policies and controls on data in line with data protection legislation (including access, protection, use and transmission).
- Take action so that policies and controls remain effective.
- Have policies to assess whether breaches need to be reported to the information commissioner (**www.ico.org.uk**).
- Maintain a cyber incident response plan in order to safely and swiftly resume operations. Learn more in **Continuity planning**.
- Satisfy themselves with service providers' controls (see **Managing advisers and service providers**).
- Receive regular reports from staff and service providers on cyber risks and incidents.

Glossary

Governing bodies

Trustees or managers of an occupational pension scheme that is subject to the requirements under section 249A of the Pensions Act 2004

Internal controls

- Arrangements and procedures to be followed in the administration and management of the scheme
- Systems and arrangements for monitoring that administration and management, and
- Arrangements and procedures to be followed for the safe custody and security of the assets of the scheme (Section 249A of the Pensions Act 2004)

Public service pension scheme

A scheme established under section 1 of the Public Service Pensions Act 2013