Guidance for trustees

Cyber security principles for pension schemes

April 2018

The Pensions Regulator

Contents

Introduction

Pension schemes hold large amounts of personal data and assets which can make them a target for fraudsters and criminals. As trustees and scheme managers, you need to take steps to protect your members and assets accordingly, which includes protecting them against the 'cyber risk'. This is an issue which all trustees and scheme managers, regardless of the size or structure of their scheme should be alert to.

The cyber risk can be broadly defined as 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. It includes risks to information (data security) as well as assets, and both internal risks (eg from staff) and external risks (eg hacking).

You should take steps to build your cyber resilience – your ability to assess and minimise the risk of a cyber incident occurring, but also to recover when an incident takes place. You should work with all relevant parties (including in-house functions, third party service providers and employers) to define your approach to managing this risk. This guide sets out good practice for pension schemes, which can be adopted proportionately to the profile of your scheme. A glossary of key terms is included at the end of this guide.

Did you know?

Internal controls are systems, arrangements and procedures for administering and managing the scheme, systems and arrangements for monitoring the administration and management of the scheme and ensuring the safe custody and security of scheme assets.

Trustees and scheme managers are required by law to establish and operate adequate internal controls to ensure their scheme is operated in accordance with scheme rules and the law. The regulator may intervene where trustees and scheme managers fail in their duties to operate adequate internal controls.

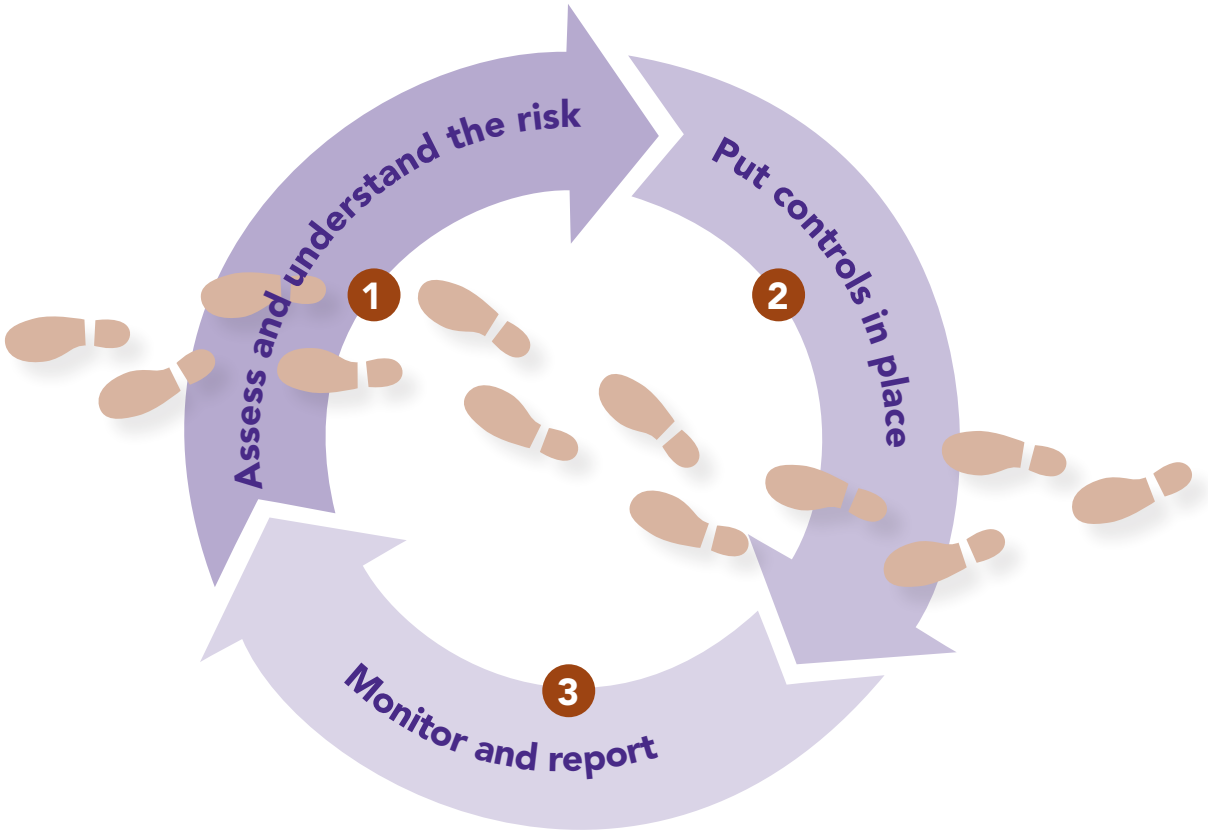
A key part of internal controls is having in place processes to identify, evaluate and manage risks. Building cyber resilience is simply one example of operating adequate internal controls.

Summary

- Trustees and scheme managers are accountable for the security of scheme information and assets
- Roles and responsibilities should be clearly defined, assigned and understood
- You should have access to the required skills and expertise to understand and manage the cyber risk in your scheme
- You should ensure sufficient understanding of the cyber risk: your scheme's key functions, systems and assets, its 'cyber footprint', vulnerabilities and impact
- The cyber risk should be on your risk register and regularly reviewed
- You should ensure sufficient controls are in place to minimise the risk of cyber incident, around systems, processes and people
- You should assure yourselves that all third party suppliers have put sufficient controls in place. Certain standards and accreditations can help you and your suppliers demonstrate cyber resilience.
- There should be an incident response plan in place to deal with incidents and enable the scheme to swiftly and safely resume operations. You should ensure you understand your third party suppliers' incident response processes.
- You should be clear on how and when incidents would be reported to you and others, including regulators
- The cyber risk is complex and evolving, and requires a dynamic response. Your controls, processes and response plan should be regularly tested and reviewed. You should be regularly updated on cyber risks, incidents and controls, and seek appropriate information and guidance on threats.

Cyber risk assessment cycle

Are roles and responsibilities clearly defined, assigned and understood?



1 Assess and understand the risk

- Do you understand the cyber risk facing your scheme:
  - your key functions, systems and assets
  - your cyber footprint, vulnerabilities and impacts?
- Is the cyber risk on your risk register and is it regularly reviewed?
- Do you have access to the right skills and expertise to understand and manage the risk?

2 Put controls in place

- Are sufficient controls in place to minimise the risk of a cyber incident occurring:
  - IT security controls
  - processes
  - people?
- Have you assured yourselves of your third party providers' controls?
- What standards or accreditations help you or your suppliers demonstrate cyber readiness?
- Do you have an response plan in place to deal with any incidents which occur and help you swiftly and safely resume operations? Do your suppliers?
- Are you compliant with data protection legislation (including readiness for the General Data Protection Regulation)?

3 Monitor and report

- Are your controls, processes and response plans regularly tested and reviewed?
- Are you clear on how and when incidents would be reported to you and others including regulators?
- Are you kept regularly updated on cyber risks, incidents and controls?
- Are you keeping up to date with information and guidance on threats?

Governance

1. You are accountable for the security of scheme information and assets, even where you delegate or outsource day-to-day functions of your scheme. You should be clear on your accountabilities, and the roles and responsibilities in respect of cyber resilience (including those of other parties such as third party providers and employers) should be clearly defined and documented. This will ensure everyone understands their role and support effective communication between relevant parties.

2. You should receive regular training and have access to the required skills and expertise to understand and manage the cyber risk.

3. You should ensure that you have sufficient understanding of the cyber risk:

    a. Understand your scheme's key functions, systems and assets (including data assets), their value to a criminal and their vulnerability to a cyber incident

    b. Understand the potential impact of a cyber incident on your scheme and, where appropriate, the sponsoring employer – operational, reputational, financial

    c. Understand the likelihood of different types of breaches occurring in your scheme, including accidental, staff-related, hacking, malware, ransomware, phishing attempts, and co-ordinated DDOS (distributed denial of service) attacks

    d. Understand the 'cyber footprint' of your scheme, ie the extent of the digital presence of all the parties involved in your scheme, and the risk posed by these parties. These can be both internal and external and include the sponsoring or participating employers, administrator, other advisers (auditor, actuaries, investment manager or consultant, lawyers), members (especially if offering online access) as well as the trustees or scheme managers themselves.

What about you?

Trustees and scheme managers themselves receive and send large amounts of potentially sensitive scheme information. You should ensure you have the right controls around your own work, eg clear policies on what can and can't be sent to personal email addresses or accessed on tablets and mobile phones.

4. The cyber risk should be included on your risk register and reviewed regularly (at least annually) and where there are substantial changes to scheme operations (eg a new IT system is put in place, or there is a change of administrator).

5. You should ensure sufficient and proportionate controls are put in place to minimise the risk of a cyber incident occurring, and reduce the impact of any that occur (set out below). You should work with all relevant parties (eg in-house functions, third party service providers and employers) to define these controls.

6. You should understand what, if anything, your internal or external auditors are looking at for you, and what is and isn't covered by any insurance you may have.

7. In some cases you may want or need to have the effectiveness of your cyber risk management independently assessed (eg by an auditor) or seek specialised accreditation, such as Cyber Essentials or ISO 27001.

8. Critically, you should assure yourselves that all third party suppliers have put sufficient controls in place to protect your member data and scheme assets:

    a. You should require suppliers to have, or adhere to, cyber security standards or good practice guides and monitor their performance. You may wish to look for information security certificates or other accreditation. You may also ask them to provide copies of relevant policies or reports (eg penetration testing reports).

    b. Cyber security should be an active consideration in the selection of a supplier and suitable provisions should be included in contracts.

9. All organisations will experience security incidents at some point, even those with the most rigorous controls. As such you should ensure an incident response plan is put in place (see below) to minimise the impact of a cyber incident.

Controls

10. IT infrastructure and security should be sufficient for the work undertaken. There should be multiple layers of security put around systems in line with the Information Commissioner's Office's (ICO) guidance on IT security (**https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf**). Where necessary you should seek expert advice on IT security.

11. Physical and virtual access to systems and data should be controlled. Staff should be suitably vetted and have just the right level of access. Access should be regularly reviewed, and closed down for leavers or where no longer relevant to a role.

12. Critical systems and data should be regularly backed up. This should include, if appropriate, one or more offline back-ups, to stop these from being affected by a cyber incident. Processes to restore backed-up data should be tested.

13. There should be a range of policies and processes in place around:

    a. acceptable use of devices (including removable and personal devices), email and internet (including social media)

    b. use of passwords and other authentication

    c. home and mobile working

    d. data access, protection (including encryption), use and transmission, in line with data protection legislation and guidance.

14. All staff, and trustees, should receive training appropriate to their role at an appropriate frequency. This should include awareness of cyber risks and how to report incidents.

15. Good monitoring is essential in order to effectively respond to incidents. Systems and networks should be monitored and logs analysed for unusual activity or unauthorised access or connections which may indicate an issue.

Incident response

16. You should have systems and processes in place to ensure the safe and swift resumption of operations. This should include an incident response plan which sets out:

    a. roles and responsibilities of the incident response team. You should ensure that your scheme has access to sufficient capability to investigate a cyber incident

    b. critical functions (eg payments of benefits) and processes, and what assurances need to be in place before these come on board

    c. in-crisis communications including how and when reporting will be made to trustees

    d. the process, thresholds and time limits for notifying other parties including the ICO, The Pensions Regulator (TPR) or the Financial Conduct Authority (FCA) as appropriate, law enforcement (in cases of fraud), third parties, and if necessary, scheme members

17. The plan should cover a range of scenarios, based on your scheme's assessment of key functions and assets, and the likelihood of different types of incident.

18. You should ensure that you understand your third party suppliers' incident processes, including how and when you would be informed of a cyber incident at the supplier.

19. Incidents should be documented and major incidents should be followed by a post-incident review. Plans should be updated in light of lessons learnt.

Final word – Dealing with an evolving risk

20. The cyber risk is complex and evolving and requires a dynamic response:

    a. controls, processes and response plans should be regularly tested and reviewed

    b. you should be regularly updated on cyber risks, incidents and controls

    c. you and other parties should seek appropriate information and guidance on cyber security threats (such as that provided by the National Cyber Security Centre), to enhance your ability to respond to, and recover from, cyber incidents. Sharing information and experiences with trusted stakeholders and peers can also be a valuable source of intelligence.

Additional links

National Cyber Security Centre

- Guidance:
  www.ncsc.gov.uk/guidance
- Threat advice:
  www.ncsc.gov.uk/threats
- Cyber essentials:
  www.cyberessentials.ncsc.gov.uk
- 10 steps to cyber security:
  www.ncsc.gov.uk/guidance/10-steps-cyber-security

Information Commissioner's Office

- Guidance on breach management:
  https://ico.org.uk/media/for-organisations/documents/1562/guidance_on_data_security_breach_management.pdf
- Guidance on IT security:
  https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf

Glossary

Cyber risk

Risk of loss, disruption or damage to a scheme or its members as a result of the failure of IT systems and processes

Cyber resilience

Ability to assess and minimise the risk of a cyber incident occurring and ability to recover when an incident occurs

Cyber footprint

The digital presence of all the parties involved in the pension scheme, and relevant outsourcers and service providers (eg Cloud service providers), which creates vulnerabilities for your scheme

Cyber incident

A breach, whether accidental or malicious, of the security rules for a system, service, process or policy

Incident response plan

A documented plan to swiftly respond to a cyber incident and enable service to resume safely and as quickly as possible.

For a full glossary of cyber-related terms, please refer to the National Cyber Security Centre guide: **www.ncsc.gov.uk/glossary**

How to contact us

Napier House
Trafalgar Place
Brighton
BN1 4DW

www.tpr.gov.uk

www.trusteetoolkit.com
Free online learning for trustees

www.pensionseducationportal.com
Free online learning for those running public service schemes

Cyber security principles for pension schemes
Guidance for trustees

The Pensions Regulator