

IIPM MARCH Webinar

20 March 2025

'DORA'



Chair



Davin Spollen
President
IIPM

Davin is Chief Executive Officer of Glennon Employee Benefits. Davin has many years' experience working in senior positions including; Director, Head of Function, Senior Consultant and Operations within regulated financial, medical and professional consultancy services firms. He has also served as Board Advisor to a Global Employee Benefits Network.

Davin is an Associate of the IIPM, Qualified Pension Trustee and Certified Financial Planner.

SAVE THE DATE

Website: iipm.ie
Email: info@iipm.ie

Next IIPM WEBINAR | Sustainability | Speaker: Ian Slattery, Zurich

Weds 7 May @ 4.45pm

ONLINE – FOLLOWING AGM @ 3.30pm

See IIPM website for registration

Speaker



John Harney

Associate Partner and Pensions DORA Specialist
Aon

John Harney is a key member of Aon's Pensions Cyber Governance and DORA Teams. A qualified actuary, John has almost a decade advising pension plans in the UK and Republic of Ireland on various aspects of strategy and governance, including cyber risk and regulatory change. John also hosts podcasts and webinars on all things pensions, as well as advocating on pension issues on LinkedIn.

AON

IIPM Webinar

**DORA for pension
schemes: Where to from
here?**

20 March 2025

4:00pm



Speakers



David Burwell
Associate Partner, Aon
Head of EMEA Pensions
Cyber Governance



John Harney
Associate Partner, Aon
Pensions DORA specialist

**Pensions specialists
working in
collaboration cyber
specialists**

**300+ schemes of all
sizes since 2016**

**Understanding of both
pensions and cyber
risk**

Agenda



The current position



Key DORA actions



Challenges



Next steps



Questions

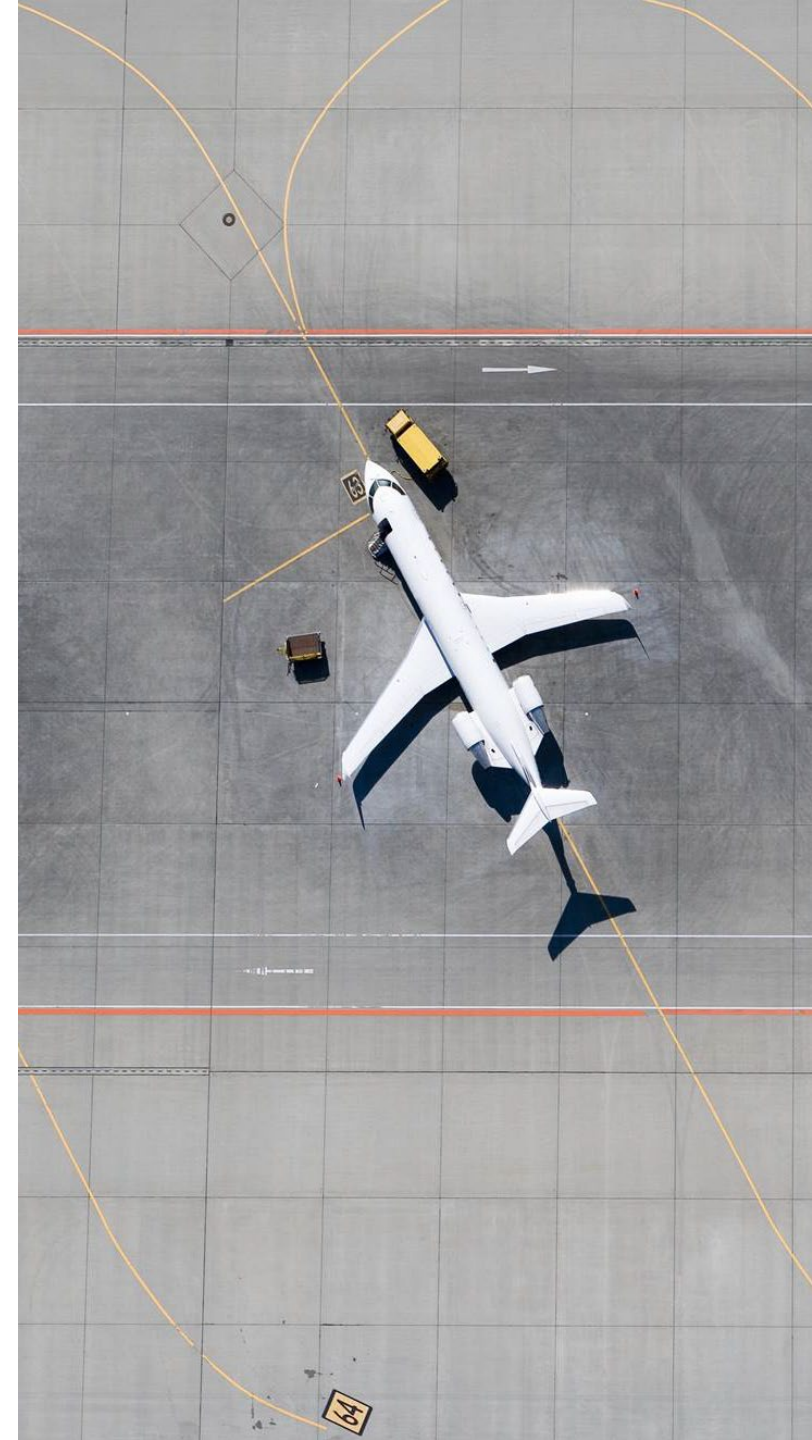
The current position

Partial
compliance

Best
endeavours

Legal &
regulatory
uncertainties

Emerging
practice



Speaker



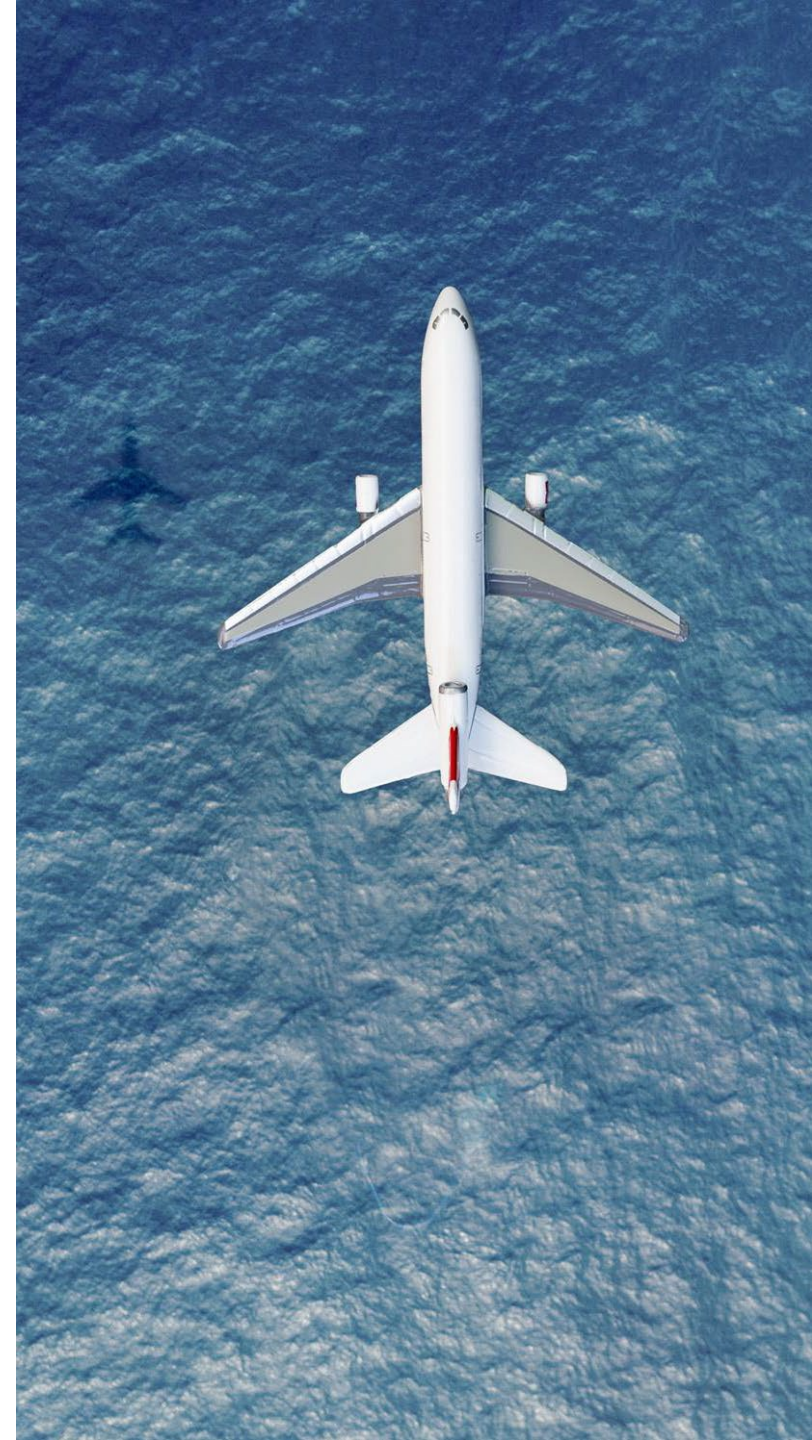
David Burwell

Head of EMEA Pensions Cyber Governance
Aon

David Burwell leads Aon's Pension Cyber Governance Team in Europe which advises over 300 pension plans on all aspects of cyber risk management. Based in London, David is a qualified actuary with over 15 years of experience in the UK and Germany. David is a regular speaker at industry events and advises the UK regulator on their cyber strategy and advice for local pension plans.

Key DORA actions

- 1** Business Continuity Planning
- 2** Register of Information
- 3** ICT risk management policy
- 4** Business Impact Analysis
- 5** Review provider(s)



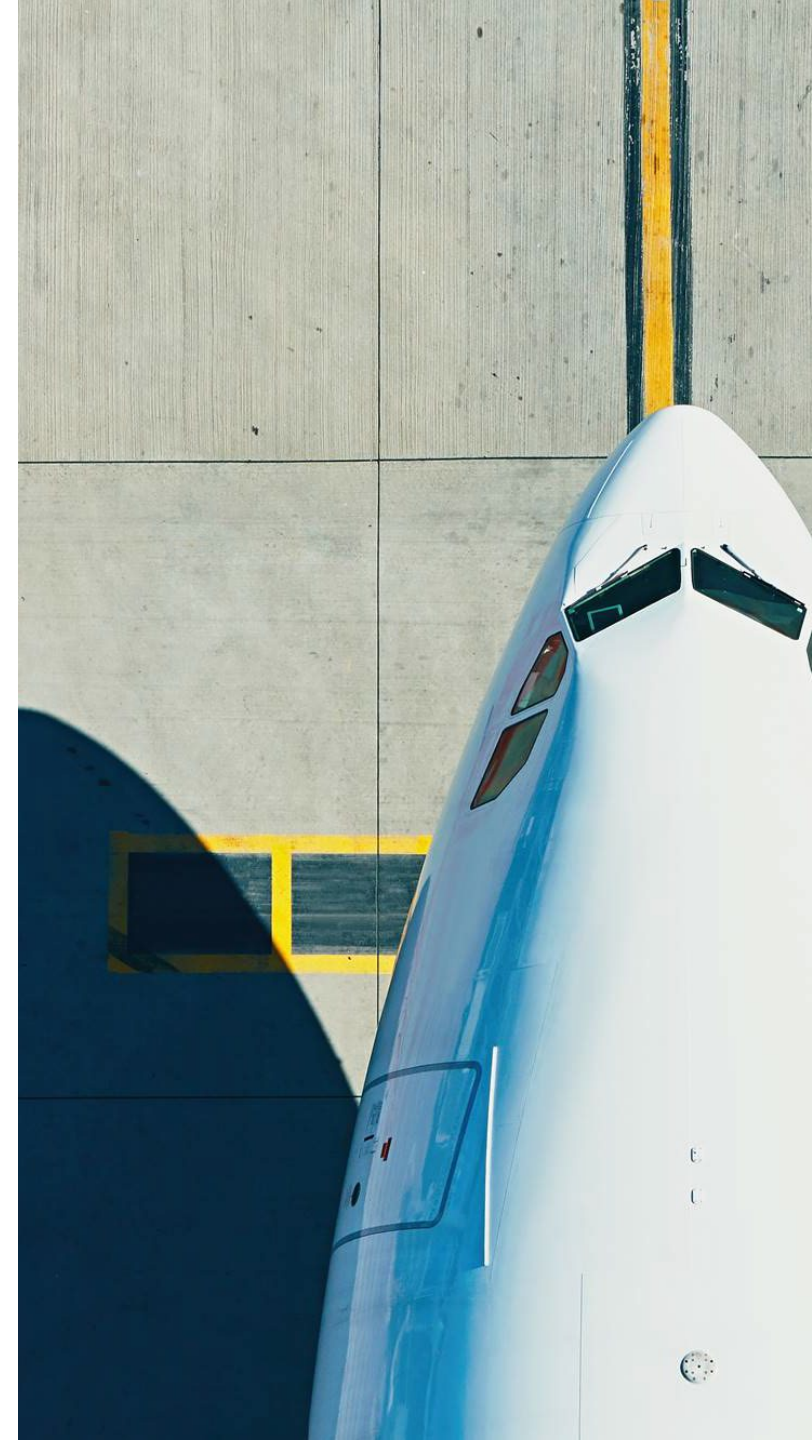
Business Continuity Planning

What is this and why is it needed?

- Trustee plan to effectively manage incidents
- Similarities to GDPR
- Testing required under a variety of scenarios
- Crisis communications
- Reporting criteria

Who involved?

- Trustees
- Specialist adviser
- Legal advisers
- Sponsor



Register of Information

What is this and why is it needed?

- Template spreadsheet
- Details ICT providers
- Critical dependencies for Pensions Authority to manage systemic risk
- Includes scheme Legal Entity Identifier (LEI)

Who carries this out?

- Schemes are responsible
- Can appoint party to submit on behalf of scheme
- Ready or submitted by 4 April 2025



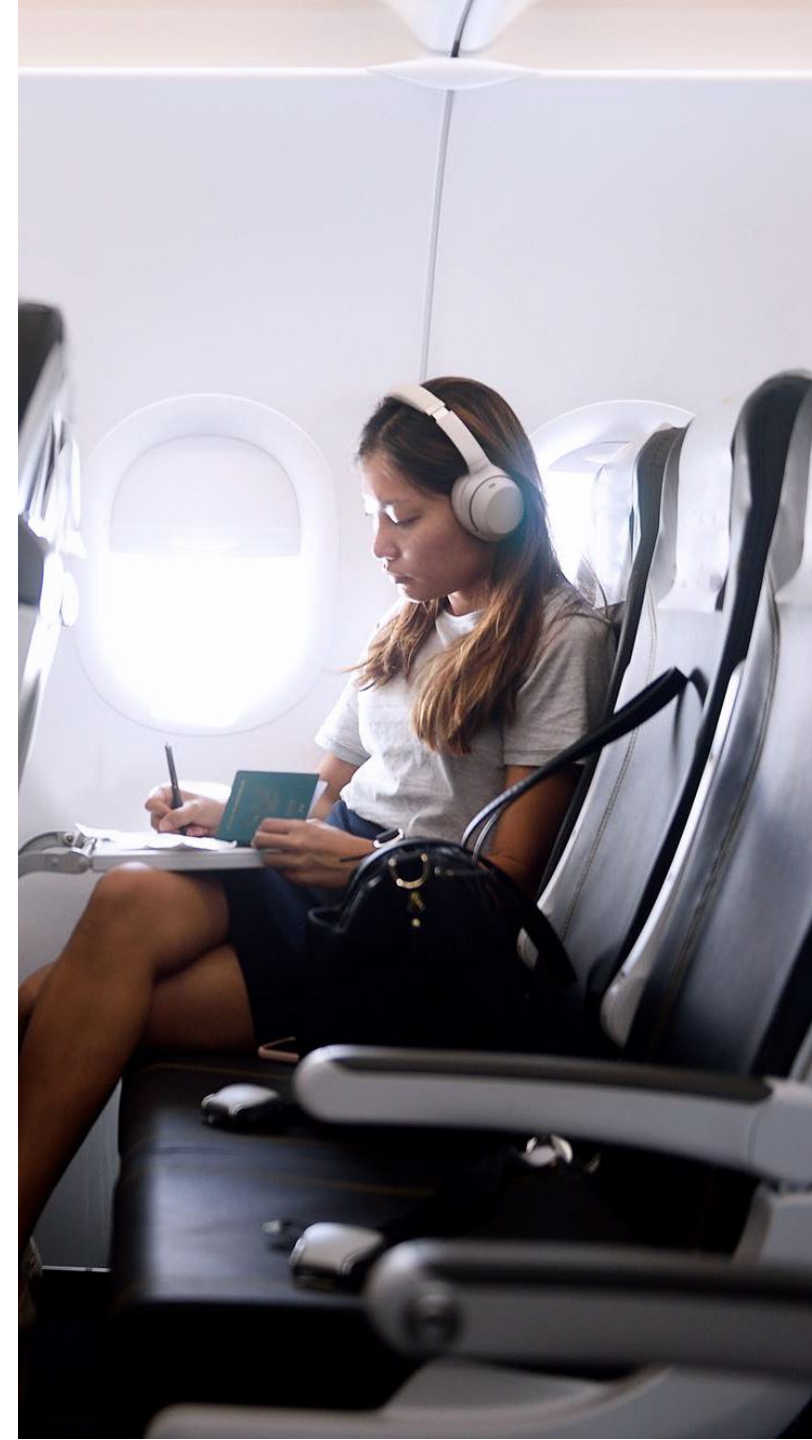
ICT Risk Management Policy

What is this and why is it needed?

- Overarching policy covering management of cyber risk
- Demonstrates how actions taken (now or in the future) mean scheme will be DORA-compliant

Who carries this out?

- Drafted by legal advisers or specialist
- Legal input crucial
- Trustee ratification and annual review



Business Impact Analysis

Scenario 1 : Data Breach

Third-party Administrator Breach, Leading to the Disclosure of Members' Data

An unpatched vulnerability in a critical third-party systems allows a threat actors to access the third-party network and exfiltrate 4,681 data records pertaining to the Fund's members.

Impacted System:

- Third Party System – A critical third party acting as a data processor for XXXXXXXXXXXX Pension Fund
- Members' Data – 4,681 data belonging to the Fund's members

Insurability Testing:

- Security & Privacy Liability

Cost Drivers:

- Member Settlements
- Legal Expenses
- GDPR Fine

The graph below aims at providing an overview of the cost drivers for this scenario:



Quantification & Insurability Analysis Overview		
Cost Category	Cost	
Crisis Expense		
Forensic	N/A*	Insurable
PR Costs	£15,000	Insurable
Notifications	£6,000	Insurable
ID & Credit Monitoring	£3,500	Insurable
Call Centre Costs	£5,000	Insurable
Extra Expenses		
Staff Overtime	£25,000	Conditionally Insurable
Cost to Improve Security Controls	£50,000	Uninsurable
Legal Expenses		
Legal – Regulatory	£25,000	Insurable
Legal – Member Settlements	£200,000	Insurable
Liability Expenses		
Member Settlements	£800,000	Insurable
Regulatory Expenses		
GDPR Fine	£100,000	Uninsurable
Regulatory Investigation	£20,000	Insurable
Total EML	£1,249,500	

* All forensic analysis will be absorbed by the third-party administrator.

■ Insurable
■ Conditionally Insurable
■ Uninsurable



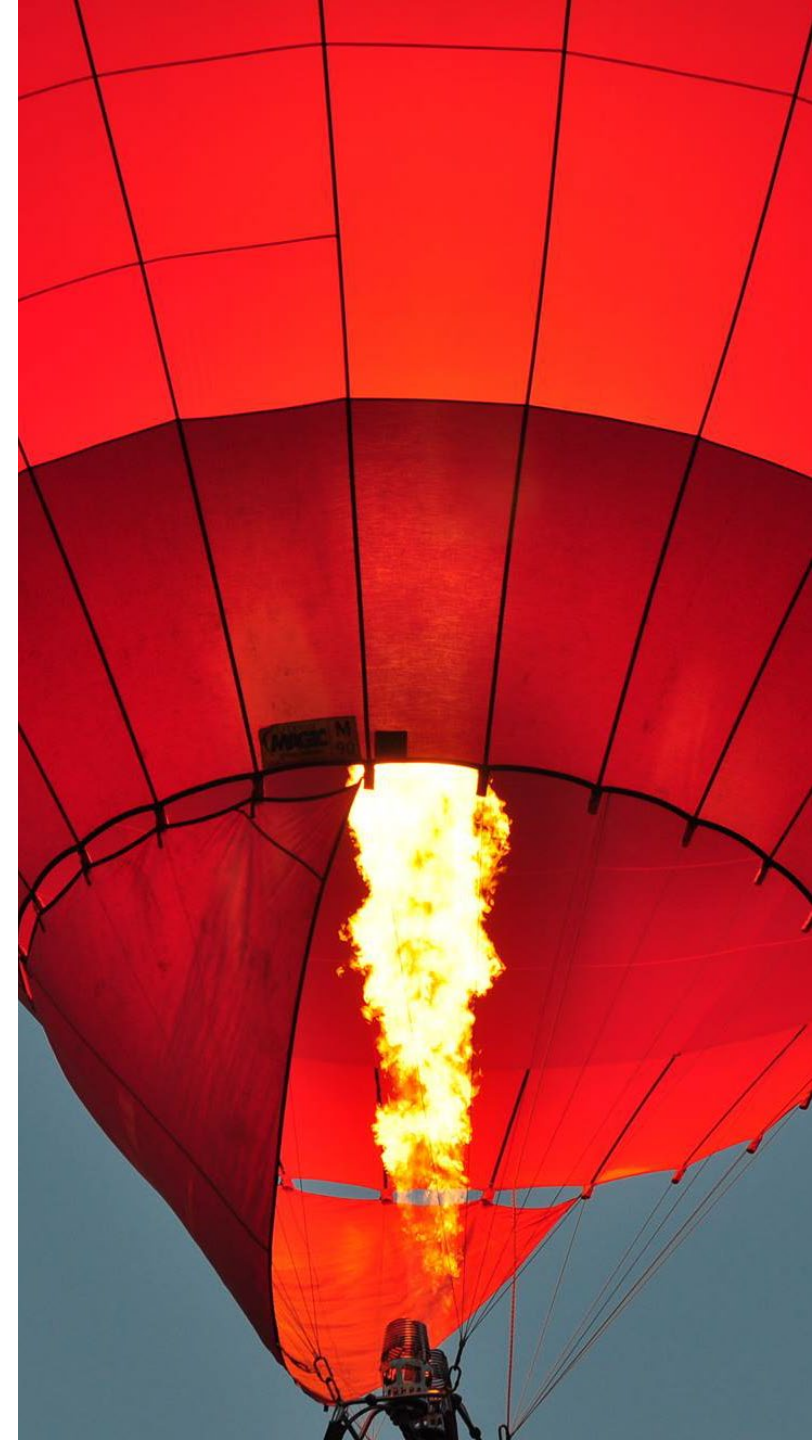
Review provider(s)

What is this and why is it needed?

- Effective risk management
- Trustees need to understand third-party ICT risk management
- Assessment of provider ICT protocols
- Ongoing process

Who carries this out?

- Trustee with support from sponsor or cyber specialist
- Sponsor's own cyber team
- Specialist technical cyber advisers



Speaker



John Harney

Associate Partner and Pensions DORA Specialist
Aon

John Harney is a key member of Aon's Pensions Cyber Governance and DORA Teams. A qualified actuary, John has almost a decade advising pension plans in the UK and Republic of Ireland on various aspects of strategy and governance, including cyber risk and regulatory change. John also hosts podcasts and webinars on all things pensions, as well as advocating on pension issues on LinkedIn.

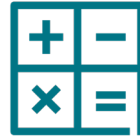
Challenges



Time



**ICT risk is
different**



**Application
to pension
schemes**



Proportionality



**Where to
start?**

Next Steps



Consider position for your Scheme



Consider gaps to DORA compliance



Talk to a specialist in pensions ICT risk management



Questions



Disclaimer:

In preparing this document we may have relied upon data supplied to us by third parties. We cannot be held accountable for any error, omission or misrepresentation of any data provided to us by such third parties (including those that are the subject of due diligence). Information in this document containing any historical information, case studies, data or analysis should not be taken as an indication or guarantee of any future performance, results, analysis, forecast or prediction. Past performance does not guarantee future results. Aon is not providing legal, financial, tax, accounting or audit advice under this document or otherwise. Should you require advice of this nature, please engage advisers specifically for this purpose.

Notwithstanding the level of skill and care used in conducting due diligence into any organisation that is the subject of a rating in this document, it is not always possible to detect the negligence, fraud, or other misconduct of the organisation being assessed or any weaknesses in that organisation's systems and controls or operations. Any opinions or assumptions in this document have been derived by us through a blend of economic theory, historical analysis and/or other sources. Any opinion or assumption may contain elements of subjective judgement and are not intended to imply, nor should be interpreted as conveying, any form of guarantee or assurance by us of any future performance. Views are derived from our research process and it should be noted in particular that we cannot research legal, regulatory, administrative or accounting procedures and accordingly make no warranty and accept no responsibility for consequences arising from relying on this document in this regard. Calculations may be derived from our proprietary models in use at that time. Models may be based on historical analysis of data and other methodologies and we may have incorporated their subjective judgement to complement such data as is available. It should be noted that models may change over time and they should not be relied upon to capture future uncertainty or events. Some of the statements in these materials may contain or be based on forward looking statements, forecasts, estimates, projections, targets, or prognosis ("forward looking statements"), which reflect our current view of future events, economic developments and financial performance. Such forward looking statements are typically indicated by the use of words which express an estimate, expectation, belief, target or forecast. These forward looking statements contain no representation or warranty of whatever kind that such future events will occur or that they will occur as described herein, or that such results will be achieved, as the occurrence of these events and any results are subject to various risks and uncertainties. Actual results may differ substantially from those assumed in the forward looking statements. We will not undertake to update or review the forward looking statements contained in these materials, whether as a result of new information or any future event or otherwise.

THIS MATERIAL DOES NOT CONSTITUTE AN OFFER OR SOLICITATION OF A FINANCIAL PRODUCT OR FINANCIAL SERVICE IN ANY JURISDICTION WHERE, OR TO ANY PERSON TO WHOM, IT WOULD BE UNAUTHORIZED OR UNLAWFUL TO DO SO. ANY SUCH PROHIBITED OFFER OR SOLICITATION IS VOID AND AON WILL DISREGARD ANY COMMUNICATION RECEIVED IN RESPECT THEREOF.

Aon plc (NYSE: AON) exists to shape decisions for the better — to protect and enrich the lives of people around the world. Through actionable analytic insight, globally integrated Risk Capital and Human Capital expertise, and locally relevant solutions, our colleagues in over 120 countries and sovereignties provide our clients with the clarity and confidence to make better risk and people decisions that help protect and grow their businesses.

Copyright © 2024 Aon Investments Limited. All rights reserved. aon.com Aon Investments Limited is authorised and regulated by the Financial Conduct Authority.

Registered in England & Wales No. 05913159. Registered office: The Aon Centre, The Leadenhall Building, 122 Leadenhall Street, London, EC3V 4AN.

The information and opinions contained in this document, enclosures or attachments (this "document") are for general information purposes only and should not be treated as a substitute for specific advice. It is based upon information available to us at the date of this document and takes no account of subsequent developments. Any reliance placed upon information in this document is at the sole discretion of the recipient. Unless we have otherwise agreed with you in writing: (a) we make no warranties, representations or undertakings about any of the content of this document and (b) Aon disclaims, to the maximum extent permissible under applicable law, any and all liability or responsibility for any loss or damage, whether direct, indirect, special, punitive, consequential (including lost profits) or any other loss or damage even if notified of the possibility of such loss or damage, arising from the use of or reliance on this document. In this disclaimer, references to "us", "we" and "Aon" include any Aon colleagues and Scheme Actuaries. To protect the confidential and proprietary information in this document, unless we provide prior written consent no part of this document should be reproduced, distributed, forwarded or communicated to anyone else. We do not accept or assume any duty of care, responsibility or liability whatsoever to any person who receives a copy of this document without our consent.



Thank you for joining us

Survey Feedback:

Please help the IIPM and complete the survey at the end of the webinar – or find the link in your follow up email

CPD DETAILS:

Attendees at the event may claim 1 hours of CPD– CPD details, link to recording and slides will be in follow up email and will be in the News section at www.iipm.ie

LIA: Not applicable for DORA | [IOB 2025-0732](#)