Appendix D

XPS
Pensions
Group

Information Security

February 2024

Information Security

XPS Pensions Group have a comprehensive information security programme designed to provide a layered defence so that all tools work together to protect both XPS Pensions Group and our clients' data.

Information Governance and Risk Management

- XPS Pensions Group are certified to ISO27001 covering all business activities provided by the Group. All information security risks are reported into a group level Audit & Risk Committee, held in a central risk register, and the committee meet on a quarterly basis to review all risks across the business. The Audit & Risk Committee report directly to the board. In addition, we hold the UK government Cyber Essentials Plus certification.
- All security policies are reviewed on an annual basis and whenever there is a policy change to ensure that they meet customer, regulatory and data protection requirements.
- XPS Pensions Group use a number of 3rd party suppliers to provide services to both clients and the business. Where these providers have access to personal data, we conduct annual security reviews.
- As part of our recruitment and on boarding process all employees are subject to vetting which includes a criminal background and credit check before they are employed, with ongoing checks against existing staff completed every two years or annually for higher risk or FCA regulated roles.
- Annual AAF01/20 audits are conducted for XPS Administration as recommended by The Pensions Regulator.

Infrastructure & Application Security

- System alerts and logs are sent to centrally managed Security Information & Event Management (SIEM) platform Microsoft Sentinel. This is monitored 24/7 by a managed security service. This service triages/prioritises security events and escalates to internal XPS security team as required.
- Site-to-site traffic is secured using SD WAN. Personal and confidential data sent externally is encrypted in transit and at rest.
- The perimeter is secured with Cisco managed firewalls, Network Security Groups (NSGs) and supplemented by a SonicWall Intrusion Detection/Intrusion Prevention System (IDS/IPS). Web facing applications are further secured by Cloudflare Web Application Firewall to protect against web threats and denial of service attacks.
- Endpoints are configured with host based firewalls to restrict traffic and further reduce the risk of lateral movement. Laptops use Windows Firewall and servers use Illumio Adaptive Security Platform.
- Network traffic is analysed using Darktrace Enterprise Immune system, a next generation AI (artificial intelligence) and machine learning technology. The system learns all traffic (patterns of life) to detect suspicious activity and Darktrace Antigena provides a recommended response to mitigate the threat.
- Email security is provided at the gateway by Mimecast Advanced Threat Prevention configured to filter incoming/outgoing mail to reduce spam, archive email and prevent attacks in malicious email attachments. This is further enhanced by Azure Advanced Threat Protection and Abnormal email security.

> Bitsight provides real time and independent security assessments against industry benchmarks.

> Abnormal provides enhanced protection against email attacks, using state of the art behavioural analysis, AI, and natural language processing (NLP) capabilities.

CYBER ESSENTIALS
CERTIFIED PLUS

Abnormal uses behavioural analysis, AI and natural language processing (NLP) to detect and automatically remediate email attacks. This is augmented by a Cofense Phishing Detection and Response platform for triaging xpsgroup.com and autonomously responding to email threats.

- Wireless Security is provided using Meraki wireless access points. Corporate networks are hidden (restricted to domain authenticated devices/users) and secured with WPA2 encryption.
- Access to the internet is controlled using Zscaler cloud-based internet proxy which blocks all access to social media, cloud-based storage, and webmail.

User Awareness & Phishing

- Security training is provided to all new joiners via KnowBe4 platform. All users are required to undertake annual refresher training.
- Bi-monthly phishing tests are conducted from KnowBe4 platform.
- Security bulletins are issued on a routine basis to provide additional security guidance and training.

Malware Prevention

- All clients and servers are configured with Microsoft Defender for Endpoint. This is AI-powered advanced threat protection designed and tested to stop Ransomware.

Data Loss Prevention Controls

- Mimecast cloud-based email security is configured for DLP and enforces encryption where explicitly required.
- Access to USB is restricted via group policy and disabled for all users by default.

Secure Configuration

- All laptops are configured with Windows 11 and are encrypted with Microsoft BitLocker.
- Regular monthly updates to servers and computer devices (e.g., laptops, PCs etc.) are implemented using Windows Server Update Service, Microsoft Intune, and Patch My PC.
- Penetration testing of our perimeter IP addresses and applications is conducted annually.
- Tenable.IO is used to conduct daily perimeter and monthly internal scans to detect and manage vulnerabilities.
- All hardware and software changes are managed through Best Practice ITIL change control processes; therefore, all changes require technical and security approval before implementation.
- Standard hardened images are used for all system builds.

Access Control

- All user accounts are controlled by Microsoft Default Domain Policy and Group Policy Objects to provide least privilege access to data and resources.
- Access is granted using the policy of ‘least privilege’ and includes regular reviews for all users.
- Accounts are secured with strong authentication and multi-factor authentication wherever possible.
- Delinea Secret Server is used for administrative password management which helps to prevent uncontrolled storage of passwords and provide easy password auditing.
- LastPass is used for password management of all non-administrative users to securely store and access credentials.

Home and Mobile Working

- Remote connectivity is secured via Microsoft AoVPN, SonicWall GVPN and Cisco AnyConnect VPNs.
- Microsoft Intune is configured to provide mobile device management (MDM) and enforces encryption on mobile devices.

Threat Intel & Monitoring

- Bitsight is used to provide an external security rating and measure ourselves against industry benchmarks.
- Quarterly threat workshops are conducted to assess cyber risks.
- Proactive threat monitoring is conducted via NCSC Early Warning System. Spiderfoot HX is used to detect indications of compromise and/or XPS data found on the internet/darkweb.

Incident Management

- Fully documented and updated Incident Management processes exist to manage security incidents which includes standing up a Cyber Incident Response Team (CIRT). Action is taken immediately following a cyber security incident or data breach. CIRT escalate all significant incidents to Incident Management Team (IMT) within 1 hour.
- Systems are backed up and replicated to Azure using Commvault and Zerto. Backup Solution can be used to recover systems if there is a virus or ransomware attack.
- BCP, DR and Cyber incident Response plans are fully implemented and tested on at least an annual basis.

For further information

If you would like further details about XPS’s approach to Information Security please contact XPS Information Security Team or your client account manager.

@xpsgroup

company/ xpsgroup

t 0118 918 5015

e it.security@xpsgroup.com

XPS Pensions Group Business Continuity Summary

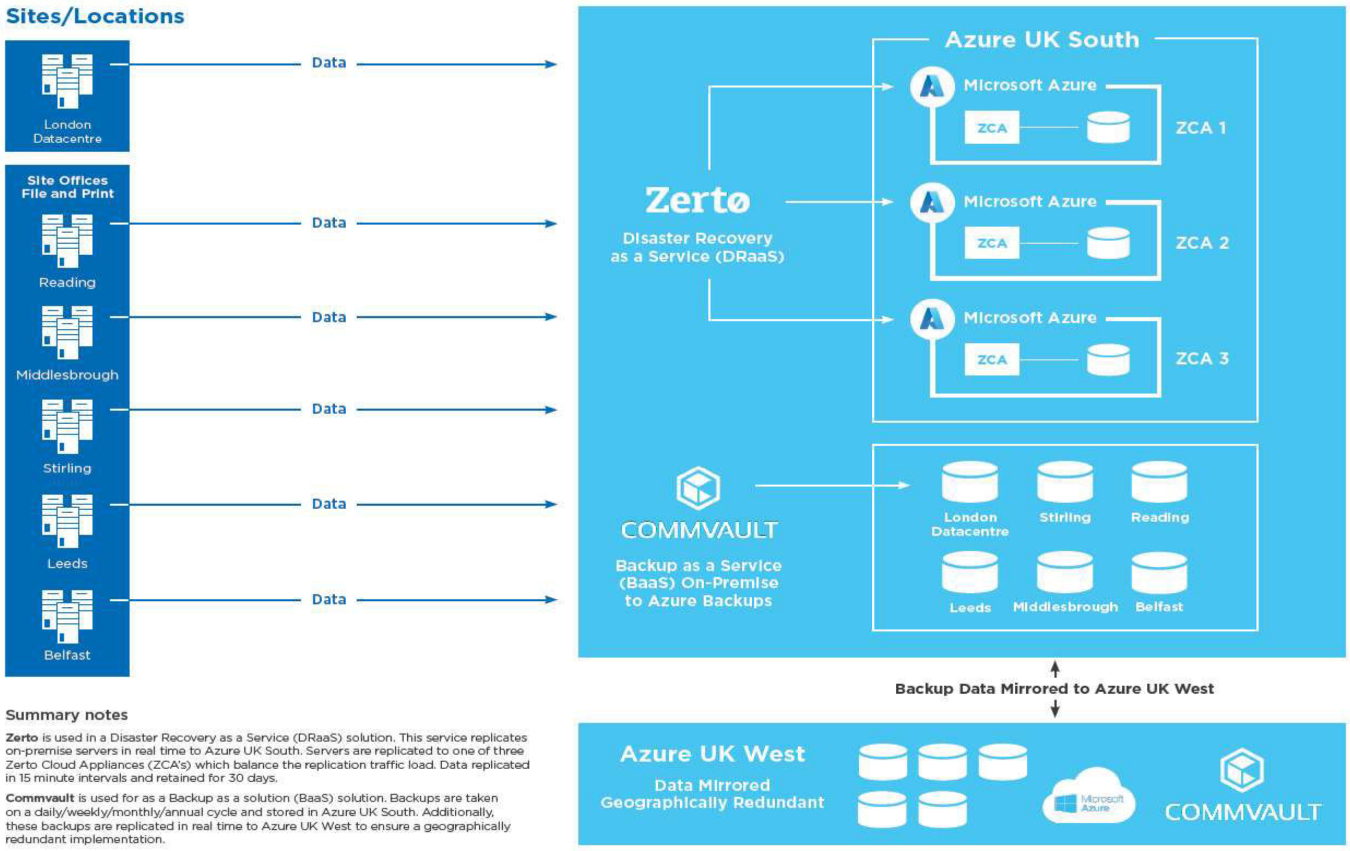
Business Continuity Management (BCM) is fundamental to the risk management strategy of XPS Pensions Group. The Board recognises that the risk of a serious unplanned interruption needs to be effectively managed. By doing this we can ensure full compliance with all regulatory requirements and maintain the level of service you, our clients, require.

BCM is managed centrally, with the Group Board, supported by the Audit and Risk Committee and the Risk Management Committee having oversight of the framework and its ongoing maintenance. Our BCM programme is aligned to ISO22301 and the Business Continuity Institute's Good Practice Guidelines. The primary objective is for all business-critical functions and processes to be prioritised and recovered within predetermined timeframes in the event of a major operational disruption.

Our Business Continuity Policy ensures that each business maintains up to date Business Recovery Plans (BRP), so that they can continue to provide all key client services if affected by a business interruption incident.

The Group currently operates using a tier three equivalent hosted data centre (DC). Our primary DC is located in London and has been designed to ensure it provides high levels of operational resilience. Data is replicated from the DC to a secondary "Disaster Recovery" Microsoft Azure tenant managed by our DRaaS partners, Databarracks. This data is replicated in near-real-time (every 5-10 secs), so were there to be an event impacting the primary DC, we can switch to the "Disaster Recovery" DC and maintain operations as normal from there with minimal interruption. Both the primary DC and the "Disaster Recovery" Azure DCs are monitored continuously to ensure that the design operates as expected, with a rolling testing program in place. This ensure they continue to deliver the capabilities required.

The chart below provides a technical overview of our DR and Backup as a Service



Summary notes

Zerto is used in a Disaster Recovery as a Service (DRaaS) solution. This service replicates on-premise servers in real time to Azure UK South. Servers are replicated to one of three Zerto Cloud Appliances (ZCA's) which balance the replication traffic load. Data replicated in 15 minute intervals and retained for 30 days.

Commvault is used for as a Backup as a solution (BaaS) solution. Backups are taken on a daily/weekly/monthly/annual cycle and stored in Azure UK South. Additionally, these backups are replicated in real time to Azure UK West to ensure a geographically redundant implementation.

When an incident impacts the Group, the Group Incident Management Team is invoked to provide strategic direction to Tactical Recovery Team(s) within the affected business area. This approach ensures strategic, prioritised recovery of critical processes, and enables clear communications to all stakeholders including our clients.

The centralised BCM framework requires plans to be reviewed and tested, and where applicable updated, on at least an annual basis. Business Recovery Plans are tested twice annually, once focusing on IT Disaster Recovery Elements and once focusing on business operations. During 2023 we have successfully completed a "Pay the Pensioner" test, our annual staff rapid notification test and additionally in September 2023 a Cyber Incident Response team test and tabletop exercise with the Plc Board. Findings from all of these tests have been recorded and actioned with enhancements to our testing plans logged and completed.

Our plans are updated following a Business Impact Assessment (BIA) which includes the identification of key personnel. Our flexible working strategy supports staff to work either from home or an office to suit business requirements, which provides a robust displacement capability in the event of any office being inaccessible for more than half a day.

We consider Business Continuity capabilities as part of our third-party selection and ongoing monitoring processes, with alternative suppliers identified for critical services wherever possible.

The Group moved to a formal flexible working environment following the pandemic with all staff issued with corporate laptops, and the ability to work from all XPS locations as well as from home. Our controls are consistent across any location with staff using VPN capabilities when working outside of an XPS office.

Scenario planning also considers new and emerging threats which may arise during the year.

For further information please contact Head of Risk

XPS Administration

Administration Update & Security

January 2024

XPS Pensions Group

We are the largest pure pensions consultancy in the UK, specialising in actuarial, covenant, investment consulting, and administration.

1,700+
Staff members

15
Locations around the UK

45
years in providing pensions advice

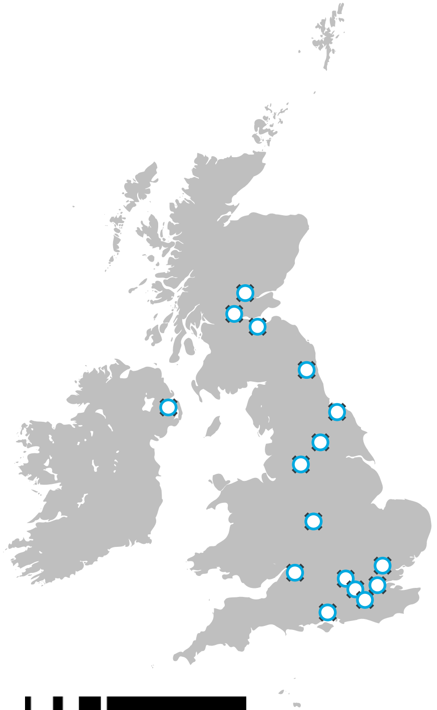
1,600+
Pension schemes and sponsoring employers

£165m
revenue p.a.

26
clients in the FTSE 250

We advise over
81
schemes with over **£1bn** in assets

90%
client-facing staff



JOHN LEWIS & PARTNERS

CompassPensions

AVIVA

PRUDENTIAL

IBM

LISTED

London Stock Exchange

XPS Administration

Long-term commitment to the administration market

We provide pensions administration to:

600+
schemes

1,022,513
members

0
services provided from outside the UK

40+
years providing scheme administration services

12
administration locations around the UK

900+
staff dedicated to administration

XPS have over 200 staff dedicated to our public sector clients administering over 300,000 members, 37 Public Sector clients covering LGPS, Police, Fire, and Ministry of Justice.

PROFESSIONAL PENSIONS UK PENSIONS AWARDS 2022 25 ANNIVERSARY
WINNER
Third-Party Administrator of the Year
XPS Pensions Group

PROFESSIONAL PENSIONS UK PENSIONS AWARDS 2021
HIGHLY COMMENDED
Third-Party Administrator of the Year
XPS Pensions Group

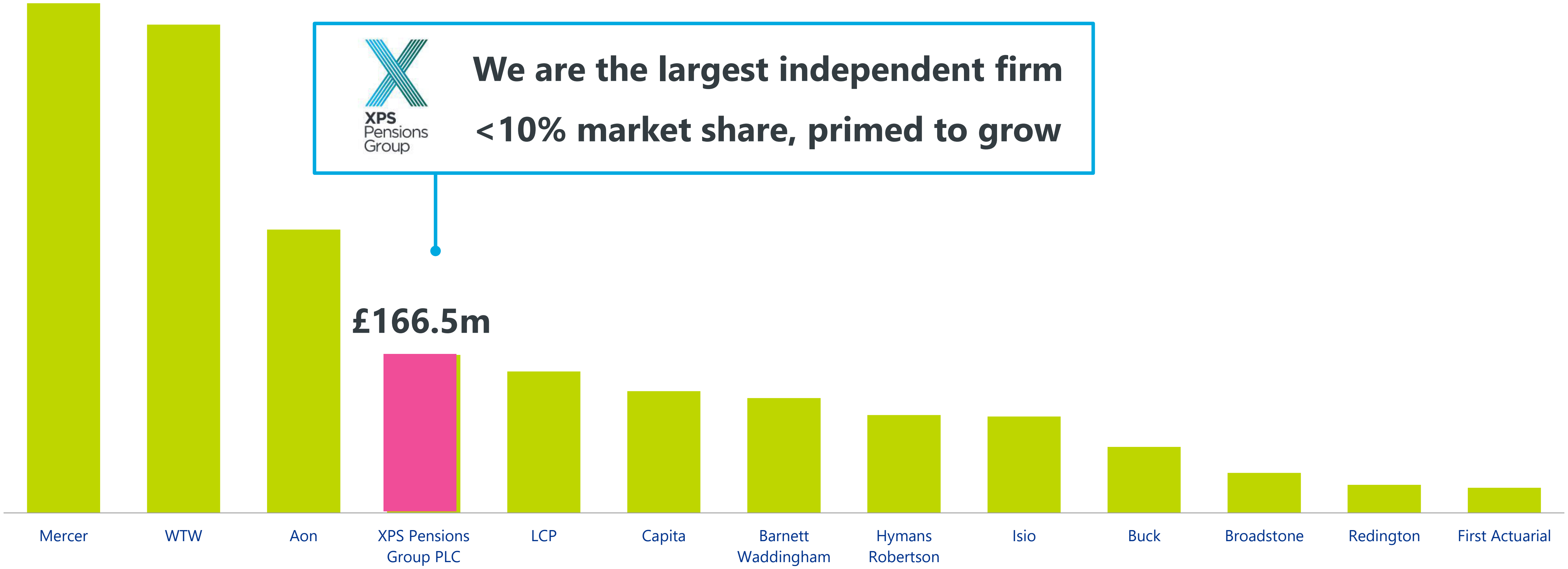
PROFESSIONAL PENSIONS UK PENSIONS AWARDS 2020
WINNER
Third-Party Administrator of the Year
XPS Pensions Group

PROFESSIONAL PENSIONS UK PENSIONS AWARDS 2019
WINNER
Third Party Administrator of the Year

No. 1 rated TPA

No.1 Third Party Administrator PROFESSIONAL PENSIONS SURVEY 2019 · 2018 · 2017 · 2016 · 2014

Market Landscape



XPS Pensions Group

We are the largest independent firm

<10% market share, primed to grow

PROFESSIONAL PENSIONS UK PENSIONS AWARDS 2022
25 ANNIVERSARY
WINNER
Actuarial/Pensions Consultancy of the Year
XPS Pensions Group

PROFESSIONAL PENSIONS UK PENSIONS AWARDS 2022
25 ANNIVERSARY
WINNER
Investment Consultancy of the Year
XPS Pensions Group

PROFESSIONAL PENSIONS UK PENSIONS AWARDS 2022
25 ANNIVERSARY
WINNER
Third-Party Administrator of the Year
XPS Pensions Group

1.8m
pieces of work a year

In excess of
450k calls

Circa 5.1m
pension payments pa

Across **38,000**
payrolls

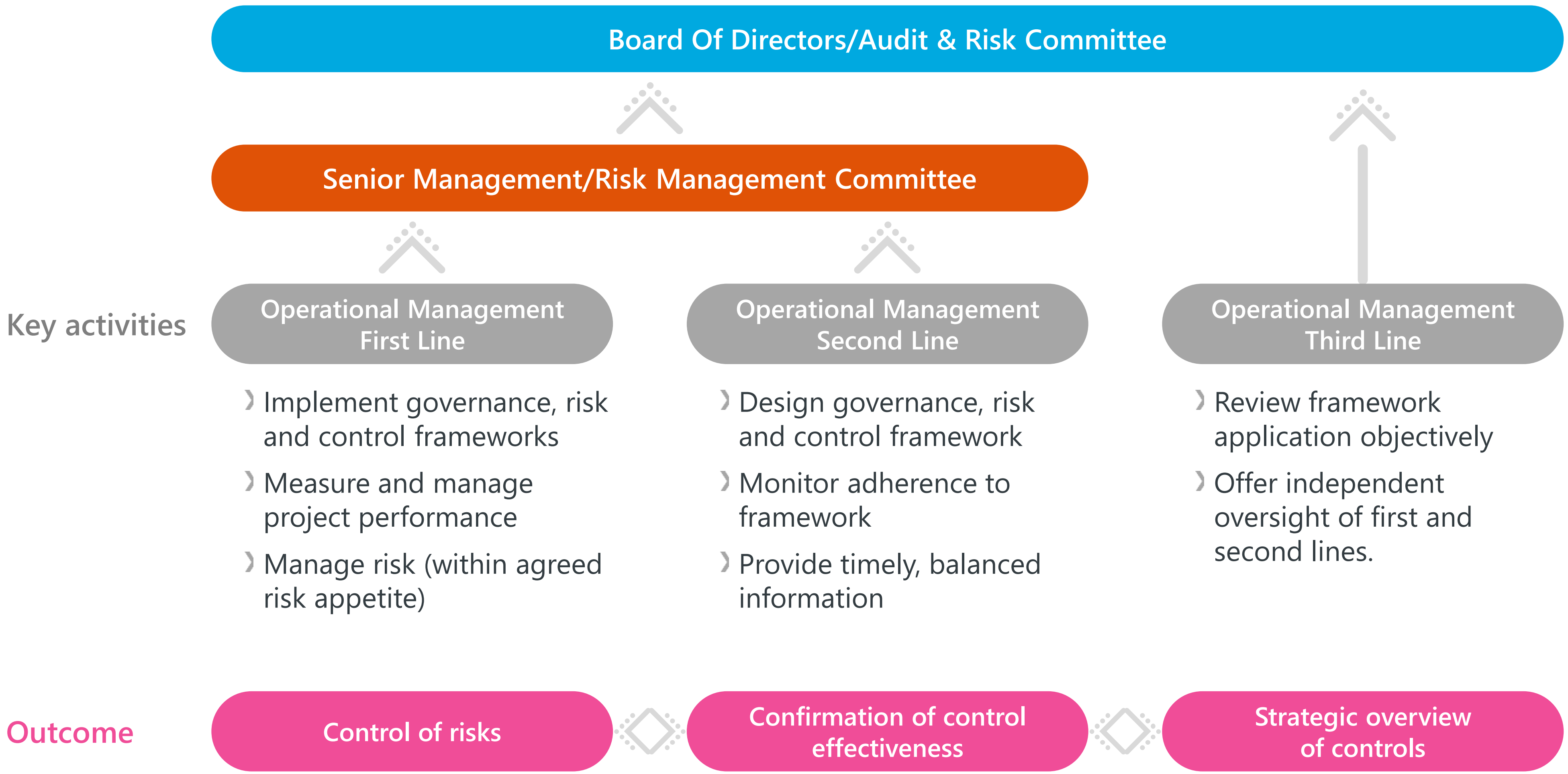
And in addition,
we protect Members
against transfer scams

3,900 transfers FY24
4% with
Regulatory Red Flags

Security

Risk Governance

- XPS Culture supports and encourages strong Risk Management as it sees it as essential to a successful business.
- Audit and Risk Committee in place with accountability to PLC Board.
- 'Three Lines of Defence Model' used to ensure risks are controlled effectively with appropriate oversight and review frameworks in place.
- Risk and Legal & Compliance Teams support second line.
- PwC currently support internal audit under co-sourced model.



Board Of Directors/Audit & Risk Committee

Senior Management/Risk Management Committee

Key activities

Operational Management First Line

- Implement governance, risk and control frameworks
- Measure and manage project performance
- Manage risk (within agreed risk appetite)

Operational Management Second Line

- Design governance, risk and control framework
- Monitor adherence to framework
- Provide timely, balanced information

Operational Management Third Line

- Review framework application objectively
- Offer independent oversight of first and second lines.

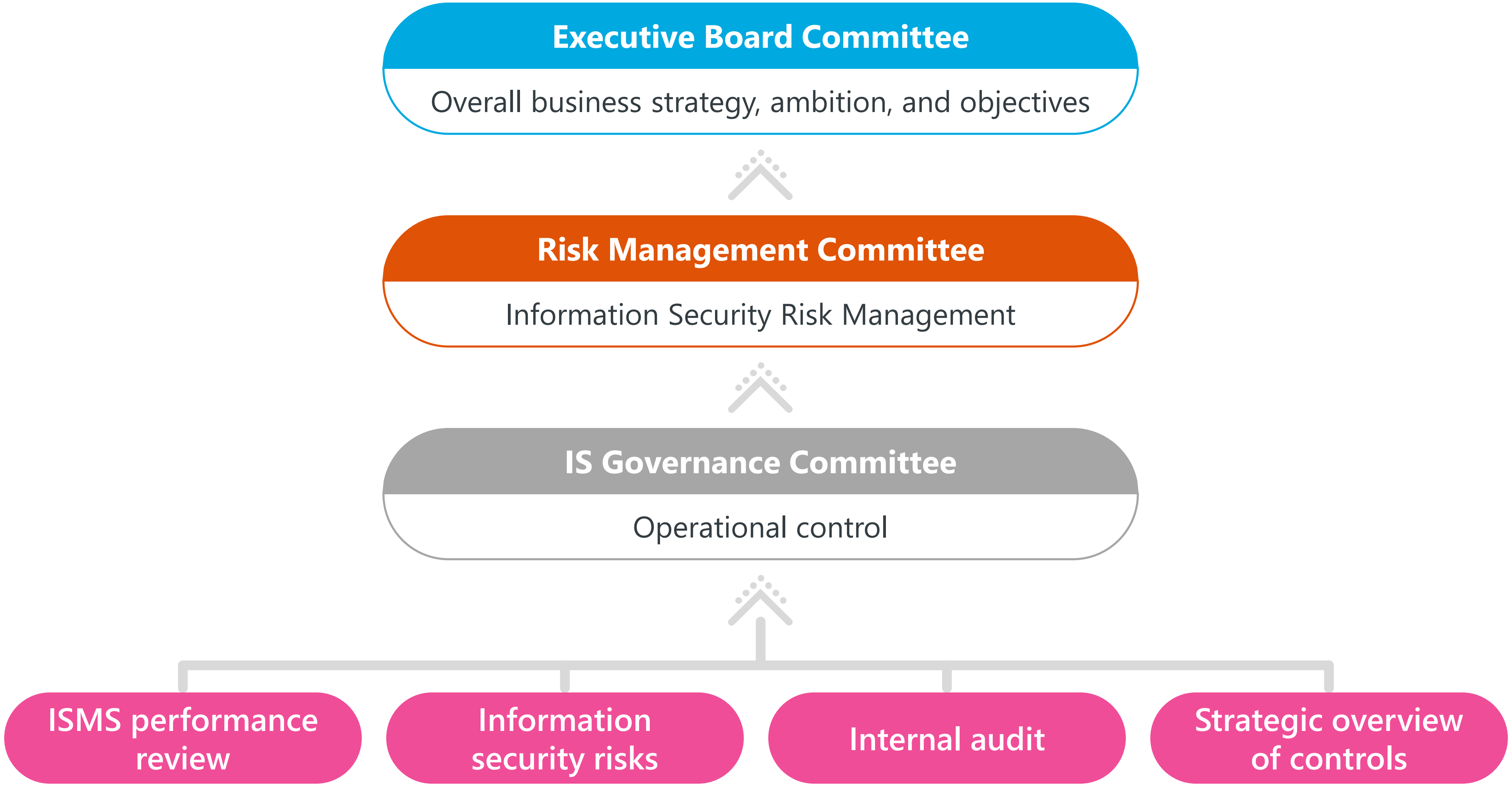
Outcome

Control of risks

Confirmation of control effectiveness

Strategic overview of controls

Information Security Governance



Executive Board Committee
Overall business strategy, ambition, and objectives
Risk Management Committee
Information Security Risk Management
IS Governance Committee
Operational control
ISMS performance review
Information security risks
Internal audit
Strategic overview of controls

Frequency:

Fortnightly

Attendees:

CIO, Head of Risk, Head of Cyber Security, IT Operations Director, Head of IT Development.

Purpose:

Oversight of cyber security incidents, cyber education, market cyber security events, cyber security projects, cyber security policy/ strategy and cyber security key performance metrics.

External certifications

LRQA CERTIFIED ISO/IEC 27001

Certified to ISO 27001:2013

Six-monthly surveillance audits by LRQA

CYBER ESSENTIALS PLUS

Cyber Essentials Plus

Annual recertification by NCC Group

ICAEW AAF 01/20

AAF 01/20 Internal controls audit

Annual audit by RSM

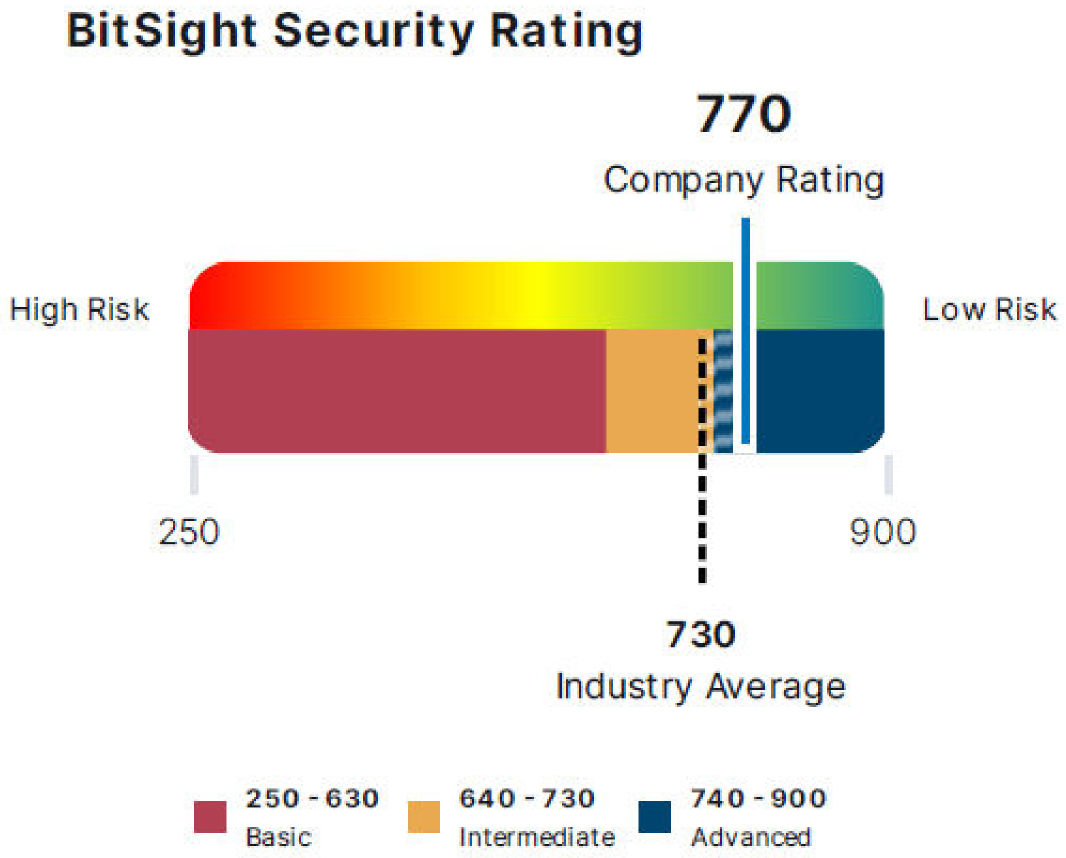
BITSIGHT

External security rating

XPS currently has a BitSight score of 770 (Advanced).

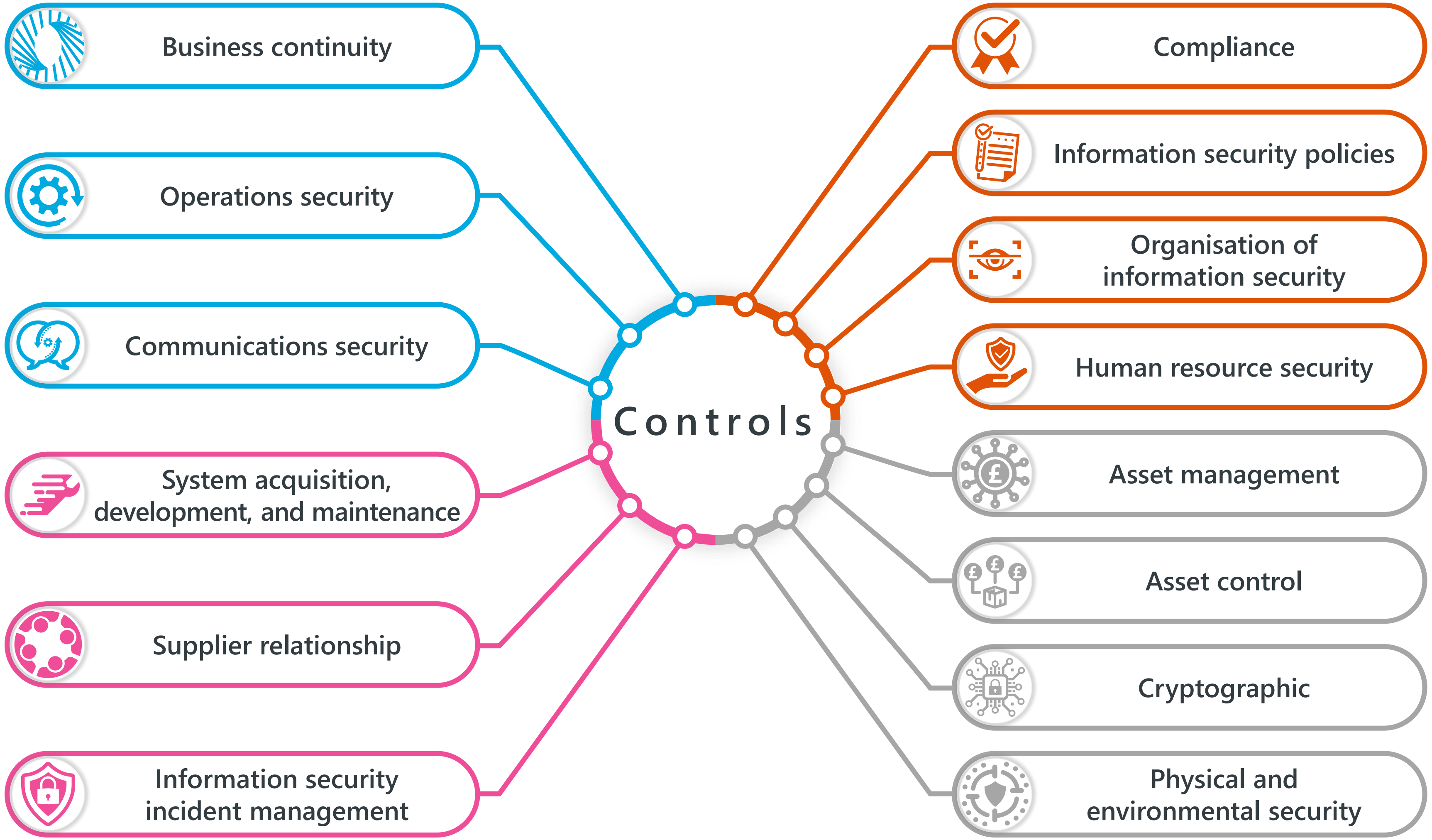
Recent ransomware attacks were at companies with a score below 640 (intermediate), many significantly lower.

- BitSight statistics:
  - Likelihood of Ransomware – Half as likely as <750 company.
  - Likelihood of Data Breach – Half as likely as <700 company.



Cyber Controls

- Recognised as a KEY RISK for Group as we pay pensions for over 450,000 people every month.
- Managed using the Information Security Management Framework aligned with the ISO27001 standard.
- Recognising the technical nature of the risk it is managed by the Information Security Steering Committee who report to the RMC and ultimately the ARC via cyber risk dashboard.
- Dedicated IT Security team supports the Defence in Depth approach used with a range of complimentary technical controls in place.
- Business continuity framework ensures requirement/capabilities reviewed and tested regularly.


Controls
Business continuity
Operations security
Communications security
System acquisition, development, and maintenance
Supplier relationship
Information security incident management
Compliance
Information security policies
Organisation of information security
Human resource security
Asset management
Asset control
Cryptographic
Physical and environmental security

Cyber Security improvements

- Renewed Cyber Essentials Plus certification in June 2022.
- Implemented BitSight and made changes to get 780 (Advanced) rating.
- Rollout of Microsoft Intune for all laptops and mobiles.
- Implemented Cloudflare Web Application Firewall for all externally facing web apps.
- Rolled out Delinea Privileged Access Management System to Security & IT Teams.
- Increased phishing testing to bi-monthly (six per year).
- Implemented Cofense – phishing detection and response platform.
- Increased internal security resources from 3 FTE to 6 FTE (Management, Engineering, and Operations).
- New DRaaS and BaaS capability implemented.

CYBER ESSENTIALS PLUS

Cyber phishing and ransomware

Our framework for protecting our information

The current risk landscape

- Significant increase in identified and prevented phishing attacks, in line with industry.
- Recognition these attacks are increasingly being used to support ransomware attacks, not just steal data.
- Response reflects need to mix people and technology controls to manage the risks.

XPS control framework

- Regular staff phishing awareness training and exercises.
- All staff now use Group issued laptops to access network via VPN and MFA implemented where possible.
- Cyber Essentials Plus Certification recertified in Q2 2022.
- Annual Purple Team Testing.
- New DRaaS and BaaS capability provides enhanced ransomware protection.
- Implementing next generation email security, e.g., behavioural analysis and natural language processing.

KnowBe4 mimecast Abnormal COFENSE TRIAGE Databarracks

Award-winning

Pensions advisory

PROFESSIONAL PENSIONS UK PENSIONS AWARDS 2022 25 ANNIVERSARY
WINNER
Actuarial/Pensions Consultancy of the Year
XPS Pensions Group

PROFESSIONAL PENSIONS UK PENSIONS AWARDS 2021
WINNER
Actuarial/Pensions Consultancy of the Year
XPS Pensions Group

PROFESSIONAL PENSIONS UK PENSIONS AWARDS 2019
WINNER
Actuarial/Pensions Consultancy of the Year

Administration

PROFESSIONAL PENSIONS UK PENSIONS AWARDS 2022 25 ANNIVERSARY
WINNER
Third-Party Administrator of the Year
XPS Pensions Group

PROFESSIONAL PENSIONS UK PENSIONS AWARDS 2020
WINNER
Third-Party Administrator of the Year
XPS Pensions Group

PROFESSIONAL PENSIONS UK PENSIONS AWARDS 2019
WINNER
Third Party Administrator of the Year

Investment

PROFESSIONAL PENSIONS UK PENSIONS AWARDS 2022 25 ANNIVERSARY
WINNER
Investment Consultancy of the Year
XPS Pensions Group

PROFESSIONAL PENSIONS UK PENSIONS AWARDS 2021
WINNER
Investment Consultancy of the Year
XPS Pensions Group

Technology

PROFESSIONAL PENSIONS UK PENSIONS AWARDS 2022 25 ANNIVERSARY
HIGHLY COMMENDED
Technology Innovation of the Year
XPS Pensions Group

Pensions expert PENSION AND INVESTMENT PROVIDER AWARDS 2020
Winner
TECHNOLOGY SERVICES OF THE YEAR
XPS Pensions Group

Culture and sustainability

Business Culture Awards 2020
Gold Overall Winner

UK EMPLOYEE EXPERIENCE AWARDS 20
GOLD AWARD WINNER
Employee Engagement

UK EMPLOYEE EXPERIENCE AWARDS 20
SILVER AWARD WINNER
Employee-centric Company

UK STEWARDSHIP CODE

Contact us

xpsgroup.com

Belfast
t 028 9032 8282
1st Floor – Flax House
83–91 Adelaide Street
Belfast
BT2 8FE

Manchester
t 0161 393 6860
Chancery Place
50 Brown Street
Manchester
M2 2JG

Birmingham
t 0121 752 6610
1 Colmore Row
Birmingham
B3 2BJ

Middlesbrough
t 0164 272 7331
Second Floor
Centre Square
Middlesbrough
TS1 2BF

Bristol
t 0117 202 0400
One Temple Quay
Temple Back East
Bristol
BS1 6DZ

Newcastle
t 0191 341 0660
4th Floor
Wellbar Central Gallowgate
Newcastle
NE1 4TD

Chelmsford
t 01245 673 500
Priory Place
New London Road
Chelmsford
CM2 0PP

Perth
t 01738 503 400
Saltire House
3 Whitefriars Crescent
Perth
PH2 0PA

Edinburgh
t 0131 370 2600
3rd Floor West Wing
40 Torphichen Street
Edinburgh
EH3 8JB

Portsmouth
t 02394 311 166
One Port Way
Port Solent
Portsmouth
PO6 4TY

Guildford
t 01483 330 100
Tempus Court
Onslow Street
Guildford
GU1 4SS

Reading
t 0118 918 5000
Phoenix House
1 Station Hill
Reading
RG1 1NB

Leeds
t 0113 244 0200
1 City Square
Leeds
LS1 2ES

Stirling
t 01786 237 042
Scotia House
Castle Business Park
Stirling
FK9 4TZ

London
t 020 3967 3895
11 Strand
London
WC2N 5HR

Wokingham
t 0118 313 0700
Albion
Fishponds Road
Wokingham
RG41 2QE

XPS Investment Limited is authorised and regulated by the Financial Conduct Authority for investment and general insurance business (FCA Register No. 528774).

This communication is based on our understanding of the position as at the date shown. It should not be relied upon for detailed advice or taken as an authoritative statement of the law.