

# REPORT ON INTERNAL CONTROLS

International Standard on  
Assurance Engagements (ISAE 3402)

For year ended 31 December 2018



APT Workplace Pensions Limited

Block B, Apex Business Centre, Blackthorn Road, Sandyford, Dublin 18

01 2063010 | [info@aptworkplacepensions.com](mailto:info@aptworkplacepensions.com) | [www.aptworkplacepensions.com](http://www.aptworkplacepensions.com)



# Contents

<b>FOREWARD .....</b>	<b>4</b>
<b>1. ABOUT US .....</b>	<b>5</b>
1.1 Background .....	5
1.2 Workplace Pension Specialists.....	5
1.3 Scale .....	6
1.4 APT Online.....	6
1.5 Employee Awareness.....	6
1.6 Senior Leaders Team.....	7
1.6 Team APT .....	9
1.7 APT Master Trust .....	9
1.8 Our Clients .....	10
1.9 Sustainability.....	10
<b>2. ASSERTION BY THE DIRECTORS .....</b>	<b>11</b>
<b>3. REPORT BY REPORTING ACCOUNTANTS .....</b>	<b>13</b>
<b>4. OUR PENSION MANAGEMENT SERVICE .....</b>	<b>16</b>
4.1 Pension Administration.....	16
4.2 Financial Administration .....	16
1.3 Trustee / Secretarial.....	17
1.4 Trustee Governance Plan.....	17
1.5 Compliance .....	17
1.6 Best Practice Standards .....	19

<b>5.</b>	<b>CONTROL ENVIRONMENT .....</b>	<b>21</b>
5.1	APT Process Control (APT PC) .....	21
5.2	Peer Review .....	21
5.3	External Audits.....	21
5.4	Workflow Management.....	21
5.4	Business Continuity.....	22
5.5	Data Security.....	22
<b>6.</b>	<b>CONTROL OBJECTIVES.....</b>	<b>24</b>
6.1	Accepting Clients.....	24
6.2	Authorisation and Processing Transactions.....	24
6.3	Maintaining Financial and Other Records.....	24
6.4	Safeguarding Assets.....	24
6.5	Monitoring Compliance .....	25
6.6	Reporting to Clients .....	25
6.7	Information Technology.....	25
6.7.1	Restricting access to systems and data.....	25
6.7.2	Providing integrity and resilience.....	25
6.7.3	Maintaining and Developing Systems Hardware and Software .....	26
6.7.4	Recovering from Processing Interruptions .....	26
6.7.5	Monitoring Compliance .....	26
6.8	Insurance Cover .....	26
6.9	Building Protection .....	26
<b>8.</b>	<b>OBJECTIVES, PROCESS CONTROLS &amp; TESTING .....</b>	<b>27</b>

## **FOREWARD**

We are pleased to present this assurance report for the fifth successive year, which describes the control environment within our pension management area.

This report has been prepared, based on the International Standard on Assurance Engagements (ISAE) No. 3402, Assurance Reports on Controls at a Service Organization, issued in December 2009 by the International Auditing and Assurance Standards Board (IAASB), which is part of the International Federation of Accountants (IFAC).

ISAE 3402 was developed to provide an international assurance standard for allowing public accountants to issue a report for use by user organizations and their auditors (user auditors) on the controls at a service organization that are likely to impact or be a part of the user organization's system of internal control over financial reporting.

A strong internal control environment is a key element in delivering high quality, risk managed pension management services to our growing portfolio of clients. This report provides information for clients and their auditors, as well as prospective clients, about how we approach the management of risk in our business, and how we operate the control environment we have in place. We believe this report demonstrates the very highest standards of reporting across the industry covering all aspects of our pension management service.

We have laid heavy emphasis on the establishment of a sophisticated IT infrastructure to enable us to handle the management of pension schemes in an efficient and compliant manner. Structuring ourselves to meet the ever-changing needs of our clients has helped us to forge sound, long-term relationships with them, many of whom have been with us for a considerable time.



**Vincent Boyle FIIPM QFA FLIA**

**Chief Executive**

**19 March 2019**

## **1. About us**

### **1.1 Background**

APT Workplace Pensions Limited (formerly known as Allied Pension Trustees Limited) was formed in 1999 and quickly established itself as a premier pensions' management firm, adding to its client base, a host of World class multinationals and indigenous companies.

Prior to the establishment of the company, the principals at APT were directors and executives of an international practice based in Dublin. This background provided APT with a unique advantage over potential competitors from the outset, i.e. an understanding of multinational employer needs combined with the dynamic of an entrepreneurial spirit.

### **1.2 Workplace Pension Specialists**

At APT we specialise in the management of workplace pensions. Our systems and infrastructure are designed to meet the ever-changing needs of our clients. We offer integrated solutions to the management of workplace pensions and specialist retirement planning vehicles. Our extensive information technology infrastructure and human resource capability combine to ensure that we are well-placed to provide a premium service to you.

Starting with the basics, we provide a robust and reliable pensions management service, to members, trustees and plan sponsors alike. This service is complemented by our financial management service which records all the financial transactions within the plan, culminating in the production of the Trustee Annual Report and Financial Statements.

Our commitment to heightening employee awareness is demonstrated in our state-of-the-art online facility -APT Online, and the series of innovative techniques employed in this endeavour. Finally, our leading-edge tailored investment solutions ensure that after all that effort, members are satisfied with their investment outcomes. Our services include:

- Plan structure and design
- Investment structures and design
- Pension administration
- Financial management and preparation of Trustee Annual reports & Accounts
- Trusteeship & secretarial services
- Legislative updates and advice

- Member awareness and advice
- Plan Governance
- Retirement counselling

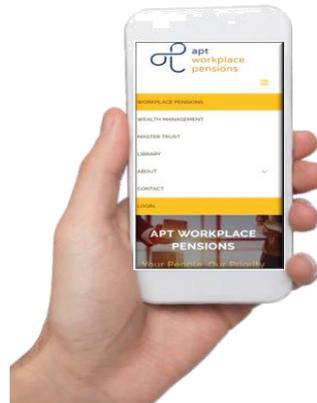
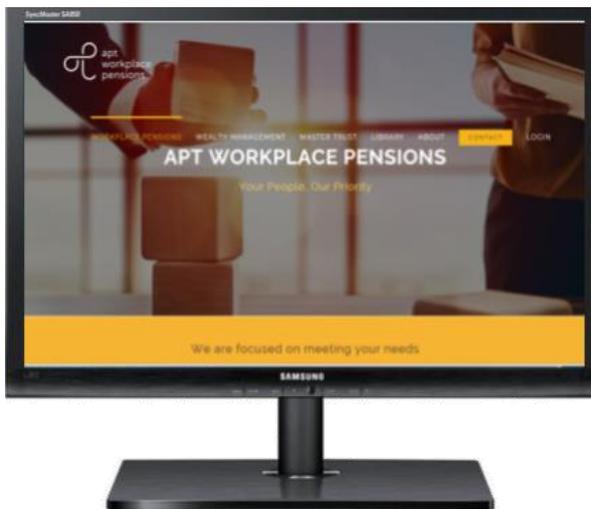
### 1.3 Scale

APT has been hugely successful in delivering pension management services to a wide variety of businesses across various industries and now manage more than €1.5bn for 55,000 members.

From our base in Sandyford, Dublin, we provide pension management services to clients in Ireland, UK and mainland Europe (under the Pan European Plan Directive - IORP).

### 1.4 APT Online

Starting with our online member portal, we bring members on a journey gradually peaking their interest in their plan over time. APT online provides a secure member portal where your members may access valuable information in relation to the pension benefits.



Members enjoy the functionality of a world class system, which allows various interactions, from fund switching, investment performance monitoring and printing of daily benefit statements.

### 1.5 Employee Awareness

At APT, we understand the importance of effective communications and education in the quest to heighten employee awareness.

Indeed, we are recognised within the industry as award-winning in each of the areas, which we believe are critical to this end.

## 1.6 Senior Leaders Team

We believe that our clients should have a dedicated resource to coordinate the delivery of services to the employer, scheme trustees and scheme members. The Senior Team responsible for the delivery of services are outlined below:-

### Vincent Boyle FIIPM QFA FLIA Chief Executive



A fellow of the Irish Institute of Pension Managers and Qualified Financial Advisor, Vincent's career stretches back over 30 years. Prior to co-founding APT, Vincent was a Director of Aon Consulting, a global employee benefit practice, operating in over 600 countries. Vincent is vastly experienced in pension matters and advises some of Ireland's largest DC pension schemes.

Vincent has overall responsibility for the delivery of services to clients. As part of this process, Vincent leads the management team in the deployment of resources and ensure that adequate measures are always in place to ensure the efficient delivery of services.

### Kirstyn Switzer QFA FIIPM Director – Administration & Online Services



Kirstyn Switzer is a founding Director and Chief Operations Officer of APT. Kirstyn will be the primary contact point for administrative and online issues.

Kirstyn is the primary contact point for administrative and online issues.

A fellow of the Irish Institute of Pension Managers and Qualified Financial Advisor, Kristyn's career stretches back over 25 years. Kirstyn is vastly experienced in all aspects of pension scheme management. Prior to founding APT, Kirstyn was Pensions Administration Manager at Aon Consulting, a global employee benefit practice, operating in over 600 countries.

Kirstyn and her team will handle the transition of schemes from incumbents. Kirstyn and her team are vastly experienced in such transitions, having migrated over 180 schemes.

### Peter Griffin QFA FLIA FIIPM – Director Member Services



A fellow of the Irish Institute of Pension Managers and Fellow of the Life Assurance Association of Ireland, Peter's career stretches back over 30 years. Peter joined as a Director of APT in 2004. Prior to that he held several senior positions with global employee benefit practices, including PWC and Aon Consulting.

As Director of Member Services, Peter leads a team of member service consultants who undertake member communications, which includes group member presentations and one to one meeting, as may be required from time to time.

Peter is a Director and Council member of the Irish Association of Pension Funds (IAPF) and is an active participant in formulating industry policy. Peter has an interest in developing pensions coverage for workers and sits on the IAPF committee that has met with the Universal Retirement Savings Development Group, an inter-departmental group chaired by the Department of Social Protection to consider the future direction of retirement savings in Ireland.

**Alex Kinsella MSc Investment & Treasury - Head of Investment Services**



Alex leads the delegated investment solutions team and is responsible for the day to day implementation of the investment strategies. Alex sits on the Investment Strategy Group (ISG) where the strategies are formally reviewed on a quarterly basis.

Alex heads up for the delegated investment solutions team

A graduate of NUI Maynooth and DCU, Alex’s career stretches back over 17 years. Alex joined APT in 2016. Prior to that he was Head Client Services in Merrion Investment Managers and previously a Portfolio Manager in Irish Life Investment Managers.

**Ollie Fahey FCCA AIIPM, APA Investment Services**



Ollie chairs the Investment Strategy Group (ISG) and brings a wealth of knowledge experience to the investment process. Ollie is a certified accountant and has over 40 years’ experience of working in the investment industry. Ollie has worked with some of Ireland’s largest investment management companies including Irish Life Investment Managers, AIB investment Managers and most recently Willis IFG.

Ollie chairs the Investment Strategy Group

**Aidan Lambe FIIPM FPMI – Trustee Service Liaison**

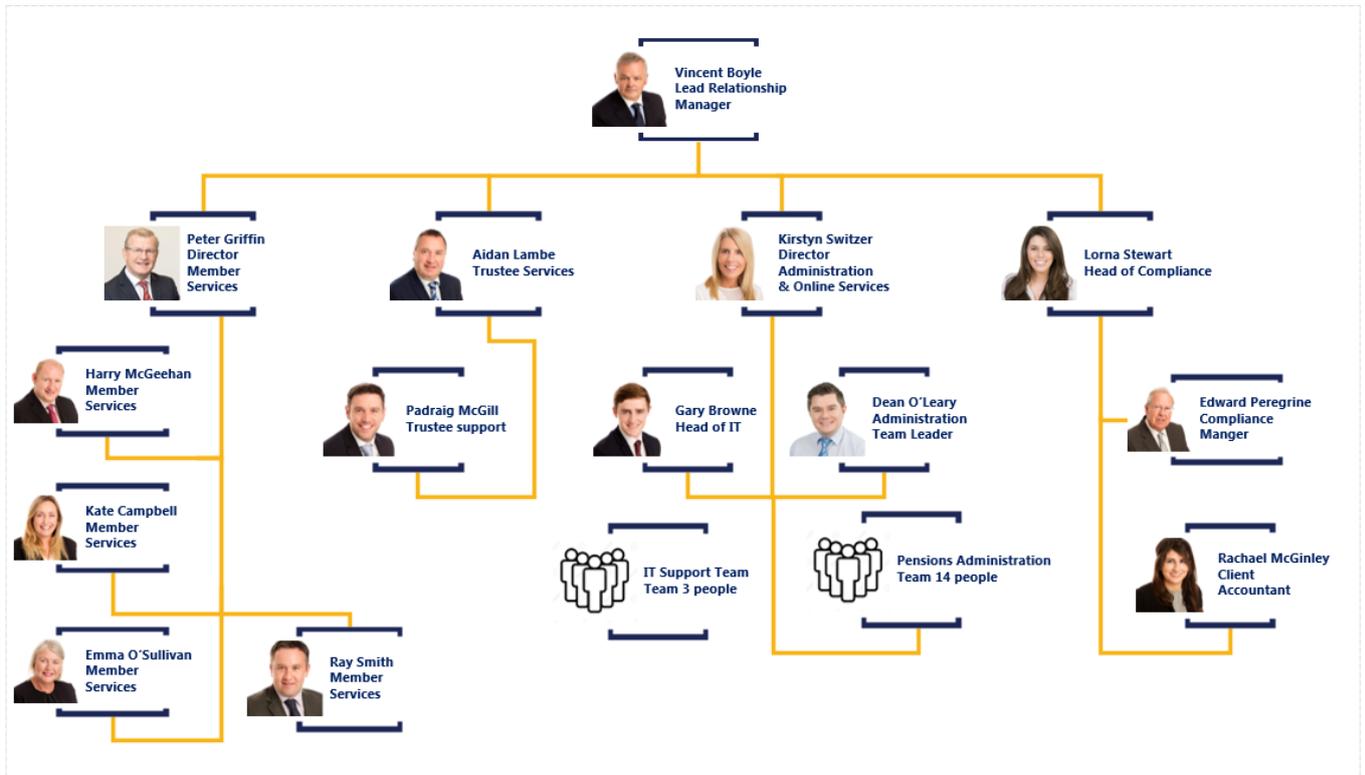


Aidan Lambe is a fellow of the Irish Institute of Pension Managers, a Fellow of the Pensions Management Institute and has over 30 years’ experience in the pensions industry. Aidan joined APT in 2003 and is head of trustee and client services. Prior to that, Aidan was a senior consultant with at Aon Consulting. Aidan fulfils the role of Trustee Service liaison to clients.

Aidan runs the Trustee Meetings and Trustee advice

## 1.6 Team APT

The organisational chart explains the roles of the wider management Team



## 1.7 APT Master Trust

The APT Master Trust was established in response to the pension reform proposals put forward by the Pensions Authority which are closely aligned with the EU Directive (IORPs II), aimed at strengthening governance risk management and transparency for occupational pension schemes. The reform proposals signal the more onerous obligations which will be imposed on Trustees under IORPs II in early 2019.

The APT Master Trust allows unconnected employers operate their pension plans under the umbrella of a single master trust. Each employer retains their autonomy in deciding the rules and benefits to apply to their workforce. An independent professional trustee board makes the key decisions around investment, governance, administration and communications and undertakes the legal and compliance responsibilities of the trust.

Moving to a master trust eases the burden of governance and compliance for defined contribution schemes by passing complete regulatory responsibility to the Master Trust Trustee, whilst

benefiting from economies of scale associated with larger groups. The advantages of the APT Master Trust are

- Reduced Risk
- Reduced Time/Cost Burden
- Economies of scale
- Value for money

### 1.8 Our Clients

Our clients extend across a broad range of both public and private sector and across various industries. An extract of our client list is shown below; -

#### Public Sector



#### Private Sector



### 1.9 Sustainability

We are conscious about the effect of our activities on society and the environment. Our commitment to quality and high standards of excellence are recognised by the Chartered Institute of Purchasing and Supply. We are a 'Rated Supplier' on the CIPS Sustainability Index. Endorsed by the Chartered Institute of Purchasing and Supply.

## 2. Assertion by the Directors

As directors of APT Workplace Pensions Limited, we are responsible for the identification of control objectives relating to the provision of pension management services by the firm and the design, implementation and operation of those controls, to provide reasonable assurance that the control objectives are achieved.

In carrying out those responsibilities we have regard not only to the interests of clients but also to those of the owners of the business and the general effectiveness and efficiency of the relevant operations.

The accompanying description has been prepared for clients who have used the pension management service and their auditors who have a sufficient understanding to consider the description, along with other information including information about controls operated by clients themselves, when assessing the risks of material misstatements of clients' financial statements.

We have evaluated the fairness of the description and the design suitability of our controls having regard to the International Standard on Assurance Engagements 3402 (ISAE 3402), issued by the International Auditing and Assurance Standards Board.

We confirm that:

- a) The accompanying description at pages 4 to 10 and 16 to 26 fairly presents the firm's pension management services from 1 January 2018 to 31 December 2018. The criteria used in making this assertion were that the accompanying description:
  - i) Presents how the services were designed and implemented, including:
    - the types of services provided and, as appropriate, the nature of transactions processed;
    - the procedures, both automated and manual, by which client transactions were initiated, recorded and processed; the accounting records and related data that was maintained, reported and corrected as necessary;
    - the system which captured and addressed significant events and conditions, other than client transactions;

- the components of the information systems supporting the relevant transactions that protected the confidentiality, integrity and availability of data;
  - and other aspects of our control environment, risk assessment process, monitoring and information and communication systems, that were relevant to our control activities; and
- ii) Does not omit or distort information relevant to the scope of the services being described, while acknowledging that the description is prepared to meet the common needs of a broad range of clients and their auditors and
- may not, therefore, include every aspect of the services that each individual client may consider important in its own particular environment.
- b) The controls related to the control objectives stated in the accompanying description were suitably designed as at 1 January 2018. The criteria used in making this assertion were that:
- i) The risks that threatened achievement of the control objectives stated in the description were identified; and
- ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved.

**Signed by the Directors of  
APT Workplace Pensions Limited**



**Vincent Boyle FIIPM QFA FLIA  
Director**



**Kirstyn Switzer FIIPM QFA  
Director**

**19 March 2019**

### 3. Report by Reporting Accountants



#### **McCloskey & Co**

Chartered Accountants & Registered Auditors

Unit B First Floor, Apex Business Centre

Blackthorn Road, Sandyford Dublin 18.

Tel: +353 1 2931069

Email: [info@mccloskeyandco.ie](mailto:info@mccloskeyandco.ie)

Web: [www.mccloskeyandco.ie](http://www.mccloskeyandco.ie)

#### **The Directors**

**APT Workplace Pensions Limited**

**Apex Business Centre**

**Blackthorn Road, Sandyford**

**Dublin 18**

#### **Dear Directors,**

This report is made solely for the use of the directors, as a body, of APT Workplace Pensions Limited, and solely for the purpose of reporting on the internal controls of APT Workplace Pensions Limited, in accordance with the terms of our engagement as reporting accountants.

Our work has been undertaken so that we might report to the directors those matters that we have agreed to state to them in this report and for no other purpose. Our report must not be recited or referred to in whole or in part in any other document nor made available, copied or recited to any other party, in any circumstances, without our express prior written permission. We permit the disclosure of this report, in full only, by the directors at their discretion to customers of APT Workplace Pensions Limited using its Pension Administration Services and to the auditors of such customers to verify that a report by the reporting accountants has been commissioned by the directors of APT Workplace Pensions Limited and issued in connection with the internal controls of APT Workplace Pensions Limited, and without assuming or accepting any responsibility or liability to customers or their auditors on our part.

To the fullest extent permitted by law, we do not accept or assume responsibility to anyone other than the directors as a body and APT Workplace Pensions Limited for our work, for this report or for the conclusions we have formed.

#### **Scope**

We have been engaged to report on APT Workplace Pensions Limited description of its administration activities throughout the period 1 January 2017 to 31 December 2018 (the description), and on the design and operation of controls related to the control objectives stated in the description.

### **Service Organisation's Responsibilities**

APT Workplace Pensions Limited is responsible for preparing the description and accompanying assertion at pages 11-12, including the completeness, accuracy and method of presentation of the description and assertion; providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

### **Service Auditors Responsibilities**

Our responsibility is to express an opinion on APT Workplace Pensions Limited description and on the design and operation of controls related to the control objectives stated in that description, based on our procedures. We conducted our engagement in accordance with International Standard on Assurance Engagements 3402, 'Assurance Reports on the Controls at a Service Organisation' issued by International Auditing and Assurance Standards Board. That standard requires that we comply with ethical requirements and plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its system, and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgement, including the assessment of the risks that the description is not fairly presented and that controls are not suitably designed or operating effectively. Our procedures including testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified by the service organisation and described on pages 27-45

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

### **Limitations of Controls at a Service Organisation**

APT Workplace Pensions Limited description is prepared to the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular environment. Also because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organisation may become inadequate or fail.

**Opinion**

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are described at page 14. In our opinion in all material facts:

- a) The description fairly presents the administration activities as designed and implemented throughout the period from 1 January 2017 to 31 December 2018
- b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 January 2017 to 31 December 2018.
- c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period 1 January 2017 to 31 December 2018.

**Description of Tests of Controls**

The specific controls tested and the nature, timing and results of those tested are listed on pages XX-



---

**Thomas McCloskey**

**For and on behalf of**

**McCloskey & Co**

**Chartered Accountants & Registered Auditors**

**19 March 2019**

## **4. Our Pension Management Service**

### **4.1 Pension Administration**

Our pensions administration capabilities are well beyond those of our competitors for both defined benefit and contribution plans. Apart from our very experienced team, our pensions administration system is delivered by Profund Solutions Limited, a specialist software provider. Built on modern technologies, it provides a scalable performant solution.

From this solid base, we provide the following pension administration tasks; -

- Maintain individual member records
- Monitor the “21 day” rule for remittance of contributions
- Undertake annual renewal of the plan
- Prepare annual benefit statement
- Prepare leaving service options and process benefit payments
- Prepare retirement benefit options and process benefit payments
- Process payments to beneficiaries in respect of death benefits
- Pensions Adjustment Orders – provide data and implement Court Orders
- Liaise with the Pensions Authority and Revenue Commissioners, as required
- Deal with matters arising from Internal Disputes Resolution (IDR) Procedures
- Deal with any matters arising from the Office of the Pensions Ombudsman
- Deal with any Pensions Authority audits
- Ensure Pensions Authority fees are paid within the statutory timeframe
- Compile the membership, contributions, transactions and investment data required to prepare the Trustee Annual Report & Financial Statements.
- Prepare quarterly administration report
- Prepare annual governance plan
- Submit Annual Scheme Information (ASI) to Pensions Authority

### **4.2 Financial Administration**

We provide a full financial administration service to the scheme to include; -

- Maintain and record all financial transactions in respect of the scheme
- Fulfil the role of paying agent on behalf of the Trustees
- Reconcile all encashment and payments through the Trustee Bank Account
- Prepare the Trustee Annual Report

- Deal with any queries from the Auditors on the back-up documentation, Trustee Annual Report or Financial Statements
- Make available to members within the statutory timeframe.

### **1.3 Trustee / Secretarial**

We act as Trustee or in some instances provide secretarial services on a stand alone basis, which include; -

- Scheduling Trustee Meetings
- Preparation of Agenda and meeting papers
- Draft minutes and action Items
- Follow up on action Items
- Present annual governance plan

At each trustee meeting we provide and present an administration report which includes; -

- Membership movements
- Analysis of inflows and expenditures
- Online usage activity
- Legislative updates

### **1.4 Trustee Governance Plan**

As part of the Trustee Secretarial and governance service, we devise Trustee Governance plans. The Governance plan sets out the annual diary of events and key areas to be addressed by the trustees to ensure the efficient and compliant management of the schemes. A Risk register is a key part of our annual governance plan. The register will include the following risks, governance & compliance, sponsor covenant, investment & markets, regulatory & legislative, and operational.

### **1.5 Compliance**

We ensure that the services we provide are consistent with the relevant regulation and best practice models, which include;

#### **A. Pensions Act 1990 (as amended)**

The key provisions of the Act as amended are listed below; -

##### **Part III Preservation of Benefits**

- Entitlement to preserved benefit DB
- Payment of preserved benefits

- Revaluation of preserved benefits
- Entitlement to transfer values

**Part IV Funding Standard**

- Actuarial Funding Standard
- Priorities on winding up

**Part V Disclosure of Information**

- Disclosure of information to members
- Annual Report & Audited annual accounts
- Actuarial valuations

**Part VI Trustees of Schemes**

- Various duties including trustee training / scheme registration and investment of contributions within deadlines.

**Part VII Registered Administrator**

- To perform the “core” duties under the Act.
- Submission of Annual Scheme Information to Pensions Authority.

**Part VIII Equal Treatment**

- Various duties including principle of equal pension treatment.

**Part VIII Compulsory & Voluntary Reporting to Pensions Authority**

- Various duties.

- **Taxes Consolidated Act 1997 (as amended)**

The Taxes Consolidation Act 1997 includes a number of provisions relating to pensions, which set out the basis on which approval of pension arrangements is established. The Revenue Commissioners (Revenue) are responsible for granting a scheme this approval, which results in the schemes having a beneficial tax status. The Taxes Consolidation Act 1997 is supplemented each year by other legislation including the Finance Act (which incorporates the government’s annual budget provisions) and is therefore amended on an annual basis.

- **The Family Law Act 1995, Family Law (Divorce) Act 1996 & Civil Partnership and Certain Rights and Obligations of Cohabitants Act 2010**

These Acts will also be relevant to the schemes in the context where a Pension Adjustment Order has been granted in a judicial separation, divorce or the dissolution of a civil partnership.

- **General Data Protection Regulations 2018 (GDPR)**

Our services are carried out in accordance with our obligations under the General Data Protection Regulations (GDPR) which came into force on 25 May 2018. From that date, the GDPR, together with applicable Irish requirements, amended existing data protection law and place enhanced accountability and transparency obligations on organisations when using personal information.

- **IORP II**

IORP II is the key European regulation for workplace pension funds, replacing the 2003 IORP Directive. IORP II enters into force in January 2019. Its scope is broad and includes Environmental, Social and corporate Governance (ESG) factors.

EU Member States were required to transpose the IORPs II Directive into national law by 13 January 2019. At the date of this publication, the Directive has not yet been transposed. It is expected that amendments will be made to the Pensions Act 1990 during the course of 2019 to bring the IORPs II Directive into force. Indeed, the Pensions Authority is currently engaging with relevant stakeholders to understand the practical issues involved and help formulate their recommendations to the Department of Employment Affairs and Social Protection in relation to the transposition of IORPs II.

## **1.6 Best Practice Standards**

The best practice standards applied to the operation of our services are ;

- **Pensions Authority**

The Pension Authority Codes of Governance issued in 2016, which are listed below; -

1. DC Code - Governance plan of action (Pensions Authority 2016).
2. DC Code - Trustee meetings (Pensions Authority 2016).
3. DC Code – Managing conflicts of interest (Pensions Authority 2016).
4. DC Code – Collection & Remittance of contributions (Pensions Authority 2016).
5. DC Code – Investing scheme assets (Pensions Authority 2016).
6. DC Code – Paying benefits (Pensions Authority 2016).
7. DC Code – Record Keeping (Pensions Authority 2016).
8. DC Code – Data Protection (Pensions Authority 2016).
9. DC Code – Risk Management (Pensions Authority 2016).

10. DC Code – Member Communications (Pension Authority 2016).

11. DC Code – Value for Money (Pension Authority 2016).

- **Pensions Ombudsman/Revenue Commissioners & Industry Best Practice.**

We have in place a robust process to ensure any complaint that may be received is dealt with in a way that should minimise the escalation to a complaint being made to the office of the Financial Services and Pensions Ombudsman.

Our scheme governance procedures ensure that plans are managed in a way that meets Revenue Guidelines. This includes review of plan benefits, checking benefits in payment and ensuring all payments from the plans are within the scheme rules and permitted by Revenue.

## **5. Control Environment**

At APT, we maintain a control environment which ensures accuracy and timeliness of work and the protection of trust assets, whilst providing sufficient flexibility at the appropriate level of seniority to meet any specific client needs. This strong control environment is achieved in many different ways, as described below.

### **5.1 APT Process Control (APT PC)**

APTPC is a series of process controls which sets out the procedures to be followed by all staff in their day to day work, including standard documents and checklists for all controlled tasks.

APTPC is maintained, updated and developed by a technical team with participants from the Management team.

### **5.2 Peer Review**

The quality of our work is paramount, and our aim is to get everything right first time. Work is therefore checked for reasonableness, accuracy and/or completeness, as well as presentation, by staff with the appropriate experience and expertise. Evidence of this checking is maintained in the casework file.

### **5.3 External Audits**

In accordance with the Pensions Act 1990 as amended, pension schemes are required to produce a set of Financial Statements and Annual Report, which are subject to audit. The financial reporting framework applied in the preparation of the statements is Irish pension's law and accounting standards issued by the Financial Reporting Council and promulgated by the Institute of Chartered Accountants in Ireland (Generally Accepted Accounting Practice in Ireland).

### **5.4 Workflow Management**

At APT we employ a workflow quality management system to keep track of routine administration tasks and to ensure that we are prepared to meet agreed or statutory reporting deadlines.

Every piece of work that arrives in our office is effectively managed using the "Therefore" system. Tasks are allocated to teams or individual administrators, their progress tracked, and all outstanding, pending, and completed tasks within the company are viewed from one location.

Working in this way places us fully in control of our administration. This enables us to have effective control over our administration work, enabling us to:

- Log work as it arrives in the office
- Monitor & track the progress of all work
- Re-allocate resources to work if required.
- Work to Service Level Agreements with set times for each stage of a process
- Run reports highlighting outstanding work, overdue work, work due shortly etc.

## **5.4 Business Continuity**

The full provisions of our disaster recovery plan are set out in our Business Continuity Plan (BCP), the purpose of which is to prepare for, respond and recover from emergencies that significantly affect the firm's ability to provide services to its customers.

The BCP addresses key elements of emergency management needed to prevent or minimize loss of personnel, product, or property and to maintain or quickly resume normal business operations following any disruptive emergency.

- It provides procedures and resources needed to assist in recovery.
- Identifies vendors and customers that must be notified in the event of a disaster.
- Assists in avoiding confusion experienced during a crisis by documenting, testing and reviewing recovery procedures.
- Documents storage, safeguarding and retrieval procedures for vital records.

### **Workplace Recovery Site**

If the BCP is invoked, key members of staff will be deployed to the disaster recovery site located at SunGard Availability Services, 5 Beckett Way, Parkwest, Dublin 12, where desks, Pc's, telephone and internet facilities are provided.

### **Microsoft Azure Site Recovery DRaaS**

From here, the team will access our Microsoft Azure Site Recovery DRaaS, where our servers and data are continuously replicated from our Sandyford existing Hyper-V infrastructure. With this real-time data replication, our Recovery Time Objective (RTO) is less than 4 hours.

## **5.5 Data Security**

The full provisions of our data security are set out in our Data Protection & IT Security Plan. In summary our data security policy includes the following components: -

- Intrusion detection and prevention based on signatures of known attacks performed at network perimeter.
- Advanced malware protection on files accessed over the Internet.
- Three tier content filtering in place preventing access to malicious and questionable web sites. Deployed on each endpoint (Panda Adaptive Defense 360), network perimeter (Cisco firewall) and DNS servers (Cisco Umbrella).
- Panda Adaptive Security 360 cyber security and anti-malware suite on all endpoints, mobile devices, servers.
- Panda Systems Management agent installed on all mobile devices with mobile device management (MDM) policy in place (includes screen lock enforcement, location and remote wipe capability).
- Anti-spam filtering is performed by Microsoft and blocks most email spam with few false positives.
- Critical Windows updates are automatically approved for installation through the group update policy.
- Data Loss Prevention (DLP) through DeviceLock DLP endpoint agent and group policy.

## **6. Control Objectives**

The following are our control objectives: -

### **6.1 Accepting Clients**

- a) Accounts are set up and administered in accordance with client agreements and applicable regulations.
- b) Complete and authorised client agreements are in place prior to starting administration.
- c) Pension schemes taken on are properly established on the system in accordance with the scheme rules and individual elections.

### **6.2 Authorisation and Processing Transactions**

- a) Contributions to defined contribution plans, defined benefit schemes, or both, and transfers of members' funds between investment options are processed accurately and in a timely manner.
- b) Benefits payable and transfer values are calculated in accordance with scheme rules and relevant legislation and are paid on a timely basis.

### **6.3 Maintaining Financial and Other Records**

- a) Member records consist of up to date and accurate information and are updated and reconciled regularly.
- b) Contributions and benefit payments are completely and accurately recorded in the proper period.
- c) Investment transactions, balances and related income are accurately recorded in the proper period.
- d) Scheme documents (deeds, policies, contracts, booklets etc.) are complete, up to date and securely held.

### **6.4 Safeguarding Assets**

- a) Member and scheme data is appropriately stored to ensure security and protection from unauthorised use.
- b) Cash is safeguarded, and payments are suitably authorised and controlled.

## **6.5 Monitoring Compliance**

- a) Contributions received in accordance with scheme rules and relevant legislation.
- b) Services are supplied to pension schemes in line with service level agreements.
- c) Transaction errors are rectified promptly, and clients treated fairly.

## **6.6 Reporting to Clients**

- a) Periodic reports to participants and scheme sponsors are accurate and complete and provided within required timescales.
- b) Annual reports and accounts are prepared in accordance with applicable law and regulations.
- c) Regulatory reports are made if necessary.

## **6.7 Information Technology**

### **6.7.1 Restricting access to systems and data**

- a) Physical access to computer networks, equipment, storage media and program documentation is restricted to authorised individuals
- b) Logical access to computer systems, programs, master data, transaction data and parameters, including access by administrators to applications, databases, systems and networks, is restricted to authorised individuals via information security tools and techniques
- c) Segregation of incompatible duties is defined, implemented and enforced by logical security controls in accordance with job roles.

### **6.7.2 Providing integrity and resilience**

- a) IT processing is authorised and scheduled appropriately, and exceptions are identified and resolved in a timely manner.
- b) Data transmissions between the service organisation and its counterparties are complete, accurate, timely and secure.
- c) Appropriate measures are implemented to counter the threat from malicious electronic attack (e.g. firewalls, anti-virus etc.).
- d) The physical IT equipment is maintained in a controlled environment.

### **6.7.3 Maintaining and Developing Systems Hardware and Software**

- a) Development and implementation of new systems, applications and software, and changes to existing systems, applications and software, are authorised, tested, approved and implemented.
- b) Data migration or modification is authorised, tested and, once performed, reconciled back to the source data.

### **6.7.4 Recovering from Processing Interruptions**

- a) Data and systems are backed up regularly, retained offsite and regularly tested for recoverability.
- b) IT hardware and software issues are monitored and resolved in a timely manner.
- c) Business and information systems recovery plans are documented, approved, tested and maintained.

### **6.7.5 Monitoring Compliance**

Outsourced activities are properly managed and monitored

### **6.8 Insurance Cover**

Suitable and up to date insurance cover is maintained.

### **6.9 Building Protection**

Access to premises is controlled

## 8. Objectives, Process Controls & Testing

1	Accepting Clients	Objective	
		Accounts are set up and administered in accordance with client agreements and applicable regulations.	
	Process	Control	Result of Accounting Testing
1.1	Standard scheme set-up documentation is reviewed by the Chief Operations Officer (COO), checking for compliance and compatibility with APT's system.	The COO signs off on the scheme information documentation checklist.	Obtained and inspected, for the selected samples, the scheme information documentation checklist for evidence of review as signed off by the COO <b>No relevant exceptions noted.</b>
1.2	Client take on is controlled through the preparation and development of a project plan by the appointed Client Service Manager (CSM).	The project plan is agreed by the implementation steering group, which comprises APT and client representatives.	For the selected sample, obtained and inspected the project plan <b>No relevant exceptions noted.</b>
1.3	Information to enable the scheme to be set up, including the Trust Deed & Rules, booklets and announcements, is gathered from the previous administrator.	The COO reviews the information received from the previous administrator for completeness. The review is evidenced by a sign off on the scheme information documentation checklist, copies of which are retained with the supporting documents. These evidences a review of items such as trust deed and rules and scheme booklets. Any outstanding documentation is added to the post go-live issues log and monitored by the COO who reports any issues to CSM	Obtained and inspected, for the sample selected, the scheme information documentation checklist for evidence of review as signed off by the Implementation Team for completeness of information from the previous administrator. <b>No relevant exceptions noted.</b>
	Accepting Clients	Objective	
		Complete and authorised client agreements in place prior to starting administration.	
	Process	Control	Result of Accounting Testing
1.4	A pension administration agreement is drawn up and authorised by the client and APT. This includes standards such as service level agreement (SLA)	A scanned copy of the Terms of Business signed by APT and the new client is filed at S:\ Company Correspondence\ Fees by the new business team. The COO checks the validity prior to accepting the client.	Obtained and inspected, for the sample selected, the letter of intent for evidence of sign off by both APT and the client.

	administration turnaround times and performance targets.		<b>No relevant exceptions noted.</b>
	<b>Accepting Clients</b>	<b>Objective</b> <b>Pension schemes taken on are properly established on the system in accordance with the scheme rules.</b>	
	<b>Process</b>	<b>Control</b>	<b>Result of Accounting Testing</b>
1.5	For Defined Benefit schemes (DB), the accuracy of data held by the previous administrator is reviewed by the COO before the live extract is uploaded to our system. Appropriate tools are used to interrogate the data and inconsistencies are reported to the client for a decision on whether data cleansing is to be undertaken. If not, the data is uploaded to our systems.	The COO reconciles the key components of the data provided by the previous administrator. Any exceptions are taken back to the ceding administrator for investigation. The reconciliation provides evidence that the data has been transferred completely from the previous administrator.	For the sample selected obtained and reviewed the reconciliations performed by the COO.  <b>No relevant exceptions noted.</b>
1.6	The COO uses a sample of test cases for each calculation type that is going to be automated on the administration system, according to the Trust Deed and Rules.	Auto-calculation results are tested against sample cases. Any discrepancies are investigated, and the testing evidenced is retained.	For the sample selected, obtained and inspected the testing evidence  <b>No relevant exceptions noted.</b>
1.7	For DC schemes member investment options are set up on the Profund system by a bulk load process in accordance with member instructions provided by the previous administrator.	Testing is carried out on DC investment member bulk loads by the COO. A selection of member records is test checked by the COO for accuracy.	For the sample selected, obtained and inspected a selection of member records for evidence of COO testing. <b>No relevant exceptions noted.</b>
1.8	For DC schemes lifestyle investment matrix options are set up on the Profund system by the COO in accordance with client instructions.	A selection of member lifestyle investment allocations and switches are test checked by the COO to the lifestyle matrix prior to the system going live. Results of these tests are reviewed to confirm that member units have been completely and accurately transferred from the previous administrator.	For the sample selected, obtained and inspected a selection of allocations and switches for evidence of COO testing and confirmation. <b>No relevant exceptions noted.</b>
1.9	For DC schemes, a unit reconciliation is undertaken between the units uploaded to our Profund system and the units held by the investment managers.	The COO undertakes the reconciliation and reports any differences to the client.	For the sample selected, obtained and inspected the reconciliations and reports.

			No relevant exceptions noted
2	Authorising & Processing Transactions	<p><b>Objective</b></p> <p>Pension schemes taken on are properly contributions to defined contribution plans, defined benefit schemes, or both, and transfers of members' funds between investment options are processed accurately and in a timely manner.</p>	
	<b>Process</b>	<b>Control</b>	<b>Result of Accounting Testing</b>
2.1	For DC schemes, all contribution data received is validated, and inconsistencies investigated and resolved by the administration team prior to the data being loaded. DC data is validated against scheme contribution investment process instructions by the administration team.	A contribution process control sheet is completed and signed off by the team to record and evidence that the contributions received are complete and no inconsistencies noted. An instruction is generated from the system and issued to the client to make payment of the money to the investment managers.	For a selection of clients, obtained and inspected process control sheets for evidence that contribution receipts had been reviewed and evidenced by sign off and on instruction generated. <b>No relevant exceptions noted.</b>
2.2	Contributions are paid directly by the client in accordance with an agreed timescale or before the 20th of the month.	The Administration Team report to scheme sponsors any potentially late receipts of contributions in the timescales agreed or before the 20th of the month.	For a selection of potential late payments, obtained and inspected evidence that potential late payments were reported to the scheme sponsors in the timescales agreed with them or in advance of the 20th of the month. <b>No relevant exceptions noted.</b>
2.3	Investments of monthly contributions are checked for accuracy at least monthly.	Contract notes are reviewed by a Senior Administrator (or other experienced administrator as appointed by the Team Manager) for units held at a specific date to ensure that the correct unit allocations are recorded on the Profund system. All discrepancies are investigated and resolved prior to sign off. This check is evidenced by the completion of the monthly contribution cycle checklist, signed off by the Administration Manager.	For a selection of clients, obtained and inspected monthly contribution cycle checklists for evidence of sign off and that checks had been performed on unit allocations to the Profund system. <b>No relevant exceptions noted.</b>
2.4	For DC pension schemes, the total investment units reported by the investment managers are reconciled to total member units held on the Profund system by	The completed reconciliation is reviewed for completeness and accuracy to ensure all units reconciled and approved at Senior	For a selection of clients, obtained and inspected investment unit reconciliations for evidence that

	investment fund at least monthly by a Senior Administrator. Any differences are investigated with the investment managers.	Administrator level or higher. This approval is evidenced by sign off of the investment unit reconciliation.	monthly checks were signed off by a senior administrator. <b>No relevant exceptions noted.</b>
2.5	Lifestyle switches for DC members are generated by a Senior Administrator on a quarterly basis and are checked and authorised by a second Senior Administrator of the team by sign off of the Profund system calculation stage. Once confirmation has been received, the first Senior Administrator updates the individual member records.	Investment instructions are reviewed by a second Senior Administrator to ensure this corresponds with adjustments required to entries held on the member's individual records as shown by system reports generated by the Profund system. This confirmation is then reviewed by the second Senior Administrator to ensure this corresponds with the Investment Instruction. The second Senior Administrator signs off the process on Profund as complete.	For the sample selected, obtained and inspected a selection of allocations and switches for evidence of COO testing and confirmation.  <b>No relevant exceptions noted.</b>
2.6	Switches requested by DC members, transfers in, transfers out and member disinvestments are processed on written request, email or notification via APT online, are completed within agreed service level agreements and are recorded as units invested and disinvested on the member's record on the Profund system by the Administration Team.	Evidence of the instruction by the member is retained on the transaction file.	For a selection of clients, obtained and inspected the transaction to ensure it was authorised by the member and that the process has been completed in Profund within the service level agreement.  <b>No relevant exceptions noted.</b>
	<b>Authorising &amp; Processing Transactions</b>	<b>Objective</b> <b>Benefits payable and transfer values are calculated in accordance with scheme rules and relevant legislation and are paid on a timely basis.</b>	
	<b>Process</b>	<b>Control</b>	<b>Result of Accounting Testing</b>
2.7	Any changes to the scheme rules impacting administration processes are documented and agreed, to enable all benefits to be paid in accordance with the scheme rules. Overall responsibility for the change is owned by the Senior Client Manager. All work is undertaken in conjunction with both the COO and administration teams using, where required, professional advisers such as the scheme actuary, to	All work is undertaken in conjunction with both the COO and Administration Teams to ensure that the amendment has been applied correctly to all environments of Profund. All benefit calculations produced for members can only be performed by a two-stage process which would check that the changes had been applied correctly. In cases where changes are required such as scheme rule changes, divorce quotes and transfer values over a certain value, sample calculations are sent to the scheme actuary	APT has stated that there were no changes to scheme rules implemented during the relevant period. As such we were unable to test the control.

	ensure that the amendment has been applied correctly.	or client for approval and sign off prior to the amendment being transferred into the live environment. All related documentation is stored in a centralised depository for future reference and referral.	<b>No relevant exceptions noted.</b>
2.8	A report is generated on a monthly basis to identify members who are six months prior to their normal retirement date. The administrator reviews the list of retirements individually and ensures the required relevant processes are set up if not already done so.	A monthly "Approaching Pension Age" report is generated by the Administration Team Manager (ATM) to identify those members who are due to reach their normal retirement date within the next six months. Options are issued to the members at their home addresses.	For a selection of clients, obtained and inspected records for evidence that reports have been run and updated to know that the process has been started and that copies have been signed off by the Administration Team Manager. <b>No relevant exceptions noted.</b>
2.9	All benefit calculation results produced for members (either automated or manual), whether generated through requests from the trustees, members or clients, are performed as a two-stage process. administration team members have process and/or authorising difficulty levels assigned to them by the Team Manager, based on their skills and knowledge.	Process authorisation levels limit administrators to doing only the processes that match the pre-set Profund difficulty levels. Assigned process and/ or authorising difficulty levels can only be approved at Administration Manager level or higher. The authorising stage checks for accuracy, legislative compliance and to ensure that the information used in the calculation is correct. This checking is evidenced by the sign off within the transaction file.	For a selection of benefit calculations, obtained and inspected calculations for evidence of allocation to correct difficulty levels and evidence of review by the correct level of authoriser. For the same selection of benefit calculations, inspected for evidence of sign off as approved by an Administration Manager level or higher. <b>No relevant exceptions noted.</b>
2.1	Calculation results and payment amounts are notified to Client Accounting for payment.	All process transactions are authorised by a second administrator and this is evidenced on the client transaction file.	For a selection of benefit calculations, obtained and inspected the transactions for evidence of review and authorisation by second administrator. <b>No relevant exceptions noted</b>
2.11	Administration processes are completed in accordance with service level agreements.	Service level agreement details are scanned to S:\Company Correspondence\Fees.	For a selection of benefit calculations, obtained and inspected evidence that the Service Level Agreements are being met. <b>No relevant exceptions noted</b>
2.12	Payments in respect of transfers out and requests for payments for transfers into the scheme are only processed by the administration team once the member's signed authorisation and documentation	All transactions are reviewed and authorised by a second administrator who checks for the receipt of all required documentation. This is evidenced on the client transaction file.	For a selection of transfers in and transfers out, obtained and inspected the client transaction file for evidence that the transactions were reviewed and authorised by a second administrator. <b>No relevant exceptions noted.</b>

	specified in the communication, including discharge forms, has been received.		
2.13	The administrator and authoriser in the administration team perform retirement processes adding and reviewing details of the pension to be paid, the date of the first payment and bank details if provided at this stage. This process is then forwarded once authorised, to the payroll team who set the pension up on the payroll system	New pensioners cannot be processed on payroll unless the retirement process has been completed. This requires the payment and pensioner details to be authorised by the administration and payroll teams. Each stage is recorded in the member's records	For a selection of new pensioners, inspected the member records for evidence that the new pensioner was processed and authorised prior to submission to payroll. <b>No relevant exceptions noted.</b>
2.14	On receipt of a notification of a death of a pensioner, their record on the Thesaurus system is ceased by the pension payroll team to ensure no further benefits are made to them.	The record amendment is authorised by a member of the Administration Team. This authorisation is evidenced by the sign off of the process on the client transaction file.	For a selection of deceased pensioners, inspected the client transaction file for evidence that the notification of death was checked and authorised. <b>No relevant exceptions noted</b>
2.15	Payrolls are processed by a dedicated Pension Payroll Team in accordance with the payroll cut-off schedule. Adjustments relating to the payroll, such as deaths, new pensioners, pension increases, are made to the system	Pension Payroll process checklists are completed to ensure all processes have been completed.	For a selection of clients, obtained and inspected pension payroll process checklists for evidence of completion. <b>No relevant exceptions noted.</b>
2.16	Members' pensions are increased in accordance with scheme requirements, (guaranteed and discretionary). Data validation checks on automated or manual calculations are coordinated by the administration team to support this.	Validation checks are signed off by the administration team Manager to confirm completeness and accuracy.	For a selection of pension increases, obtained and inspected evidence that the validation checks, were completed and signed off. <b>No relevant exceptions noted.</b>
<b>3.</b>	<b>Maintaining Financial and Other Records</b>	<b>Objective</b> <b>Member records consist of up to date and accurate information and are updated and reconciled regularly</b>	
	<b>Process</b>	<b>Control</b>	<b>Result of Accounting Testing</b>
3.1	The creation of new member records and member data changes as advised by the client or member are	Any amendment to existing data or sets of new member records is checked by an administrator against the source, which is either scanned to the member record or detailed on the interface file	For a selection of new member records and data changes, inspected members records for evidence that the validation checks were undertaken prior to

	subject to validation checks by the Administration Team prior to processing.	and is authorised by a second administrator. This authorisation is evidenced by the sign off of the process within the client transaction file.	the processing and for evidence that the processes were signed off by a second administrator. <b>No relevant exceptions noted.</b>
3.2	Scheme data, including member details, salary and contribution information, is kept up-to-date through periodic data loads from the employer's payroll and HR information systems. New data is validated within the Profund system interface process and once correct is authorised and loaded onto the database by the Administration Team.	Once the data has been validated within the Profund system interface process, in order for data to be uploaded or go live, the upload must be authorised by another member of the Administration Team, which can be evidenced in the process control sheet.	For a selection of data uploads, inspected data received for evidence that it had been validated, authorised and loaded onto the database. This was evidenced via inspection of the process control sheet showing that a peer review was completed. <b>No relevant exceptions noted.</b>
3.3	Within the data upload process, error messages are generated from error reports produced if the data is clearly incorrect or incomplete.	Discrepancies are investigated by the Events Team and/or Pension Administration Team, as necessary, and resolved. System configuration is such that the data upload process cannot be completed until errors are resolved.	For a selection of clients, obtained and inspected error reports for evidence of investigation and resolution by the events team and/or pension administration team and observed that the system did not allow the process to be completed until the errors were resolved. <b>No relevant exceptions noted.</b>
3.4	All contributions for DC schemes are entered into a scheme specific register (Profund register). The contributions are then checked against the Schedule of Contributions/payment schedule, employer's remittance ad- vice/Excel	A contribution schedule is completed for checking of contributions to the Schedule of Contributions/payment schedule, remittance advice or Excel spreadsheets from the employer. Discrepancies identified are investigated with the client. The check is evidenced by the sign off on the process control sheet.	For a selection of DC contribution receipts, inspected the scheme- specific contribution schedule and the remittance from the employer for evidence of cross-checking of accuracy and sign off. <b>No relevant exceptions noted.</b>
	<b>Maintaining Financial and Other Records</b>	<b>Objective</b> Investment transactions, balances and related income are accurately recorded in the proper period.	
	<b>Process</b>	<b>Control</b>	<b>Result of Accounting Testing</b>
3.5	Investment purchases, sales, investment income and changes in investment valuation are analysed and reconciled by the Client Accountant on a quarterly/	Journals are reconciled and authorised by the Client Accountant preparing the journal.	For a selection of clients, obtained and inspected the accounting journals for evidence of being prepared and authorised by the Client Accountant.

	annual basis from investment manager or custodian statements. The Client Accountant prepares the journal to include the transactions in the nominal ledger and reconciles the results.		<b>No relevant exceptions noted.</b>
3.6	All journal entries into the accounting system other than receipts, payments, bank charges and interest (which are entered from bank statements) are supported by journal forms that have been authorised by a Client Accountant. The Client Accountants review the nominal ledger as required when preparing quarterly cash forecasts, management accounts and annual financial statements.	Journals can only be posted to Sage if authorised by the Client Accountant.	For a selection of clients, obtained and inspected journal entries for evidence of authorisation by the Client Accountant.  <b>No relevant exceptions noted.</b>
3.7	Original deeds, policies and contracts are held by the clients, but copies are maintained for all the documents supplied by the client. These are securely held electronically on our network or in paper files on site.	Client permanent files are maintained electronically and kept in restricted access drives and APT online. At client request, significant original paper files are stored in secure locked cabinets in restricted access areas and are retained for trustee secretarial purposes only.	Through observation and enquiry, evidenced that the client permanent files are kept in restricted access drives, and original paper files are stored in locked cabinets.  <b>No relevant exceptions noted.</b>
3.8	Where required, secure off-site facilities are used for the storage of client paper files.	Archived paper files are held with a recognised storage company and an agreed retention/destruction schedule is in place.	Through observation and enquiry, evidenced that a retention/destruction schedule had been agreed between APT and the storage provider.  <b>No relevant exceptions noted.</b>
<b>4</b>	<b>Safeguarding Assets</b>	<b>Objective</b> <b>Member and scheme data is appropriately stored to ensure security and protection from unauthorized use</b>	
	<b>Process</b>	<b>Control</b>	<b>Result of Accounting Testing</b>
4.1	Setting up of scheme bank accounts is authorised by pension scheme trustees, and changes to bank account mandates require authorisation by two APT Executives. Accounts are held on behalf of Trustees	Any bank account set up or change to the account signatories requires authorisation by at least two trustees and two APT Directors. This authorisation is evidenced by a sign off on the Third-Party Mandate by at least two Executives (in accordance with the authorised signatory list).	For a selection of bank accounts, obtained and inspected copies of the mandates for evidence that changes to the account were signed by two APT Directors.

	under a Third-Party Mandate, whereby APT operate the accounts on their behalf.		<b>No relevant exceptions noted.</b>
4.2	Incoming cheques are recorded on receipt and are banked on the same day. Cheques that are not banked that day are either returned to the issuer or passed back to the Client Accounting Team and stored securely	Daily cheque listings are completed by administration team and reconciled by the Client Accounting Team to cheques received for banking to ensure that all cheques received are accounted for. Any discrepancies are reported to the administration teams and investigated. The cheques are not banked until these discrepancies are resolved.	For a selection of cheques received in the period obtained, the daily cheque list, for evidence that these were reconciled by the Client Accounting Team and any discrepancies reported to the Administration Teams and investigated. <b>No relevant exceptions noted.</b>
4.3	Cash transactions are monitored by the Client Accounting Team on a daily basis to ensure that all cash transactions are recorded onto the accounting system.	Monthly bank reconciliations are undertaken by the Client Accounting Team for some schemes, with results stored on the Sage system. At month end a final reconciliation is completed, reviewed and signed off by a member of the Client Accounting Team. Any differences are investigated by the Client Accounting Team so that the reconciliations balance (i.e. incorrect postings) will be amended or missed entries will be actioned.	For a selection of clients, inspected the accounting system for evidence of monthly bank reconciliations being completed by the Client Accounting Team. For a selection of months, obtained and inspected reconciliation reports for evidence that bank statements had been reconciled to the accounting system and that these monthly reconciliations were reviewed and signed off by a member of the Client Accounting Team. <b>No relevant exceptions noted.</b>
4.4	At least two members of staff are involved in the release of any payment.	Cheque and electronic payment initiation forms are separately raised and approved. Authorisation is in accordance with the established authority mandate. System restrictions within the Banking on line and cheque production systems prevent the initiator of a payment from authorising or releasing it.	A selection of payments were inspected for evidence that initiation forms are separately raised and approved in accordance with the established authority mandate. Through observation and enquiry, checked that the banking online initiator of a payment could not authorise or release it. <b>No relevant exceptions noted.</b>
<b>5</b>	<b>Monitoring Compliance</b>	<b>Objective</b> <b>Contributions received in accordance with scheme rules and relevant legislation.</b>	
	<b>Process</b>	<b>Control</b>	<b>Result of Accounting Testing</b>

5.1	The administration team record receipt of all contributions received. In the case of DC contributions, they advise the administrator when payment is outstanding. Checks are run in accordance with the requirements under the Pensions Act 1990 and trustee practise for each scheme e.g. for most schemes the cashier checks payments have been received by 20th of the month.	Administrators are advised which contributions are outstanding and follow up action is taken if necessary, by the administrator. The administrator will pursue the employer for payment.	Obtained and inspected potentially late contributions for evidence that follow up by the administrator.  <b>No relevant exceptions noted.</b>
5.2	Day to day work is logged on to the workflow management system and logged off when completed.	Deadlines are monitored by the administrators to ensure they are met. Regular reports are produced at both a team and management level in order to ensure that standards are being maintained.	Obtained and reviewed reports to evidence that deadlines are being met in line with SLA's. <b>No relevant exceptions noted.</b>
5.3	Service Level Agreement (SLA) requirements are monitored regularly for each client by the COO who measures actual performance against these requirements.	Service level requirements for contractual and disclosure service standards are reviewed for quarterly performance against agreed targets and provided to clients in regular administration reports.	For a selection of clients obtained the performance review information for indication of compliance with SLA requirements. <b>No relevant exceptions noted.</b>
	<b>Monitoring Compliance</b>	<b>Objective</b> <b>Transaction errors are rectified promptly, and clients treated fairly</b>	
	<b>Process</b>	<b>Control</b>	<b>Result of Accounting Testing</b>
5.4	The administrator checks transactions to ensure that they are in accordance with relevant instructions. The administrator will ask the manager to rectify any transaction issues in a timely manner. If an error is discovered during the course of an audit this must be raised with the manager.	For DC schemes the Profund reconciliation report will highlight any issues. Once any issues have been resolved the reconciliation report is re-run by the administrator and checked to ensure it agrees. The COO will ascertain whether there has been any material loss to the client and authorise payment if required.  All errors or complaints are recorded by the team leader on the errors and complaints database.	For a selection, obtained and reviewed Profund reconciliations for issues detected and their subsequent resolution and review by the COO. Also reviewed the errors and complaints database to ensure prompt and fair resolution.  <b>No relevant exceptions noted.</b>
5.5	Administration reports, which may include membership movement analysis and reconciliations, are produced on the basis and frequency as agreed with the scheme trustees. Where requested by the	The reports are checked for completeness and accuracy and peer reviewed prior to being issued. Scheme annual events are monitored on a regular basis by the administrator.	For a selection of clients checked the reports for evidence of checking and review.

	trustee's quarterly administration reports are produced and distributed to scheme trustees		<b>No relevant exceptions noted.</b>
5.6	Benefit statements are produced annually from data held on the administration system and are dispatched within timescales agreed with trustees.	Checks are conducted in accordance with the benefit statement procedure and signed off by a supervisor	For a selection of clients ensured the benefit statement had been checked and signed off. <b>No relevant exceptions noted.</b>
<b>6</b>	<b>Reporting to Clients</b>	<b>Objective</b> <b>Annual reports and accounts are prepared in accordance with applicable law and regulations.</b>	
	<b>Process</b>	<b>Control</b>	<b>Result of Accounting Testing</b>
6.1	Annual report and accounts are prepared in compliance with the latest Statement of Recommended Practice (SORP) for pension schemes based on a standard reporting format. The accountant updates the standard reporting format to take into account any changes in legislation. Annual accounts are prepared and then checked by a supervisor prior to audit. Audited accounts once approved are signed off by the trustees.	Deadlines for the finalisation and approval of audited accounts are monitored by administrative and accounting staff on a regular basis.  A control sheet detailing progress and accounts deadlines is monitored regularly by the accounts manager and any necessary action is taken. The report is circulated to the Team Leaders and COO monthly for information.	For a selection of clients, obtained and inspected the accounts for evidence of peer review and sign off by the Client Accountant, to ensure that accounts are prepared in compliance with the latest SORP for pensions schemes.  <b>No relevant exceptions noted.</b>
6.2	Documented internal procedures are followed by administrators who log all breaches in the breaches log and notify management and the COO	Reports are made as necessary to the COO. The COO will assess and refer where necessary to the Board.	Obtained and inspected the breaches log to ensure all breaches are reported to the COO. <b>No relevant exceptions noted.</b>
<b>7</b>	<b>Information Technology</b>	<b>Objective</b> <b>Physical access to computer networks, equipment, storage media and program documentation is restricted to authorised individuals</b>	
	<b>Process</b>	<b>Control</b>	<b>Result of Accounting Testing</b>
7.1	Formal documented Information Security policies and procedures are in place to cover aspects of Information Security including physical access, system backup and access control.	Formal documented Information Security policies and procedures are in place to cover aspects of Information Security including physical access, system backup and access control.	Inspected IS Security Policy and noted that it covered aspects of Information Security including physical access, system backup and access control.

			<b>No relevant exceptions noted.</b>
7.2	The Sandyford server room is protected against damage, and equipment is maintained at optimal operational conditions.	The Sandyford server room is equipped with raised floors, climate control and smoke detectors. The temperature and humidity levels are monitored on working days by a member of the IS Helpdesk Team.	Inspected the computer room area and noted that it was equipped with raised floors, climate control and smoke detectors. Inspected the temperature and humidity monitoring system. <b>No relevant exceptions noted.</b>
7.3	Access is approved to a limited number of IT Operations staff only and there are several physical and logical controls in place to prevent unauthorised access. On premises server and network equipment to support any local services IPS specific applications are located in secure server rooms accessed by key fob. Use of key is by authorised individuals. Keys and key codes are authorised by the ITS Operations Manager and restricted to authorised individuals. Authorised individuals can admit others (e.g. engineers) but will continuously supervise them.	All office entrants and exits are locked, and access is by key cards / fobs issued to staff. Visitors have restricted access. Access cards to the APT Building is restricted and provided as part of the induction process of a new employee. Upon an employee leaving the organisation, notifications are sent from HR to IT Services to notify them that access needs to be removed.	Access cards to buildings are only granted upon notification from HR. Access for additional hours must be provided by management. Access is disabled within a timely manner of the employee leaving the company and is initiated by HR/Building services. Inspected the reports detailing the access rights and ensured users are added and removed on a timely basis. <b>No relevant exceptions noted.</b>
7.4	IPS specific applications are located in secure server rooms accessed by key fob. Use of key is by authorised individuals. Keys and key codes are authorised by the ITS Operations Manager and restricted to authorised individuals. Authorised individuals can admit others (e.g. engineers) but will continuously supervise them.	Access cards to buildings are only granted upon notification from HR. Access for additional hours must be provided by management. Access is disabled within a timely manner of the employee leaving the company and is initiated by HR/Building services.	<b>No relevant exceptions noted.</b>
7.5	Uninterruptable power supply (“UPS”) provides an alternative source of power in the event of disruption to the electrical supply.	The UPS load in Sandyford is checked on a weekly basis and recorded on the weekly checklist by IT department.	For a selection of weeks, inspected weekly checklists. <b>No relevant exceptions noted.</b>
7.6	Laptops are encrypted and configured to have password protections on boot before issuing.	All laptops and desktops are configured to enforce encryption on any portable media device inserted.	Tested a selection of devices for encryption on portable media devices. <b>No relevant exceptions noted.</b>

Information Technology		Objective	
Process		Control	
Process		Control	
Process		Result of Accounting Testing	
7.7	Access to core applications and the system network is controlled through unique User IDs and passwords. Password strength protocols are enforced for access to the system network and key applications to prevent unauthorised access to user network accounts. Users must regularly change their system network and key application passwords.	To gain access to core applications and the system network, users must authenticate themselves with their unique User ID and password. Access controls include: <ul style="list-style-type: none"> <li>• A set minimum characters in length for passwords</li> <li>• Automated system controls on the network and key applications force users to change their password at least every 42 days</li> <li>• User accounts are locked after three unsuccessful access attempts.</li> <li>• These are logged and must be reset by system administrators</li> <li>• User workstations are locked automatically after a ten-minute period of inactivity and require the logged in user's ID and password to unlock.</li> </ul>	For a selection of accounts, inspected the network and application settings and noted that users were either unable to access the accounts or the accounts had been set up as read only. Inspected the password parameters for the network and key applications and noted that passwords were set to be a minimum of eight characters in length. It was also noted that users were automatically forced to change their passwords at least every 42 days and that user accounts are locked after three unsuccessful access attempts.  Enquired regarding the lockout of user accounts and was informed that locked out users were required to contact the helpdesk to be reset. Inspected the password parameters for network accounts and noted that user workstations were locked automatically after ten minutes of inactivity. Observed a locked workstation and noted that a password was required to unlock the workstation.  <b>No relevant exceptions noted.</b>
7.8	Access to the system network and applications is restricted to authorised individuals.	The appropriate line manager or application owner must approve the access request prior to access being granted.	Inspected a selection of access requests for new joiners to the network and key applications and

			noted that approval had been obtained from line managers. <b>No relevant exceptions noted.</b>
7.9	Accounts are disabled or deleted on a timely basis when an individual leaves employment or changed where an individual change their role.	HR notify IT of leavers prior to them leaving. User accounts are disabled or deleted by the IT department in line with the received notification.	For a selection of leavers from the organisation, noted that access to the network and key applications had been disabled or deleted in a timely fashion. <b>No relevant exceptions noted</b>
7.10	Remote access to the system network and key applications is approved before being granted	Remote access requests are logged on the Helpdesk system and are approved by the CEO.	For a selection of users granted remote access in the period, ensured they had been approved by the CEO <b>No relevant exceptions noted.</b>
	<b>Information Technology</b>	<b>Objective</b> Segregation of incompatible duties is defined, implemented and enforced by logical security controls in accordance with job roles.	
	<b>Process</b>	<b>Control</b>	<b>Result of Accounting Testing</b>
7.11	IT privileged access rights are segregated across the IT Team such that no one individual has pervasive access.	Privileged IT access rights are segregated across the IS Team. Through the review of printouts of user access rights, all IT privileged access is reviewed on a quarterly basis by the IT Manager and a relevant Director in the business.	For a selection of quarters noted that access had been reviewed and signed off as authorised by the Head of IT. <b>No relevant exceptions noted.</b>
	<b>Information Technology</b>	<b>Objective</b> IT processing is authorised and scheduled appropriately, and exceptions are identified and resolved in a timely manner.	
	<b>Process</b>	<b>Control</b>	<b>Result of Accounting Testing</b>
7.12	IT processing is scheduled to avoid interruptions in the processing schedule.	IT processing is carefully scheduled by the IT Manager and COO to occur outside of core processing hours. Special projects are scheduled and agreed with the COO.	Reviewed the IT schedule to ensure that events are timed to cause minimum disruption to processing. <b>No relevant exceptions noted.</b>

	<b>Information Technology</b>	<b>Objective</b> Data transmissions between the service organisation and its counterparties are complete, accurate, timely and secure.	
	<b>Process</b>	<b>Control</b>	<b>Result of Accounting Testing</b>
7.13	Our primary web server, secondary web and application servers are located at SunGard System's Limited Parkwest Business Park, Clondalkin, Dublin 22, a "state of the art" data centre which operates 24 / 7 with complete support systems including intruder detection monitoring.	Virtual Private Network (VPN) Data is transmitted between our Sandyford and SunGard servers at intervals during the day using the VPN tunnel on Cisco infrastructure. All transfer of data through the VPN is encrypted.	Reviewed the data transmission procedures to ensure that data transfers through VPN are encrypted.  <b>No relevant exceptions noted.</b>
7.14	Transmissions of data to and from clients are made via a secure website facility. End users may only make changes to the underlying database and master files via the front-end applications.	Direct access to business data is restricted to SQL Programmers and Sys Admin and DBA users	Examined the access rights to ensure that direct access to business data is restricted.  <b>No relevant exceptions noted.</b>
	<b>Information Technology</b>	<b>Objective</b> Appropriate measures are implemented to counter the threat from malicious electronic attack (e.g. firewalls, anti-virus etc.).	
	<b>Process</b>	<b>Control</b>	<b>Result of Accounting Testing</b>
7.15	Security patches (i.e. periodic vendor-supplied software updates designed to address identified security issues) are applied to workstations as appropriate.	Security patches are tested by the IS Projects Manager prior to being released and applied to workstations.	Reviewed the testing log to ensure new patches are tested prior to being applied.  <b>No relevant exceptions noted.</b>
7.16	Servers and workstations are protected against virus infection.	Antivirus software is used throughout our network. Forefront security is used for mail filtering, together with an external spam filter. Open DNS is used for malware protection and internet policy enforcement. Anti-virus software is installed on servers in Sandyford and all workstations. The anti-virus software and	For a selection of months, inspected reports showing anti-virus software update history for servers and PCs and noted that the reports provided software update history for servers and PCs and identified those where the definition was not up-to-date. For a

		updates are centrally managed. The virus definition distribution is checked on a monthly basis by the IS Manager to identify instances of non-compliance, which are then investigated and resolved.	selection of identified instances of non-compliance, inspected definition files and noted that they had been investigated and resolved. <b>No relevant exceptions noted.</b>
7.17	A unified threat management (“UTM”) firewall protects the internal network from unauthorised access from external systems, including the Internet, and intrusion detection sensors are deployed. Firewall activity logs are reviewed on a monthly basis by the IS Projects Manager.	Cisco ASA firewalls are installed on our network at SunGard Systems and Sandyford. As part of this security measure, we use restrictive port filtering to minimise the opportunity of attack.	For a selection of months, inspected reports of firewall activity, and noted that they had been reviewed by the Head of IT.  <b>No relevant exceptions noted.</b>
	<b>Information Technology</b>	<b>Objective</b> <b>The physical IT equipment is maintained in a controlled environment</b>	
	<b>Process</b>	<b>Control</b>	<b>Result of Accounting Testing</b>
7.18	<p>Critical IT infrastructure is located in an offsite data centre. Access is approved to a limited number of IT Infrastructure staff only by the IT Manager.</p> <p>Secure data storage providing an independent copy of all data held in the offsite data centres is located in a secure computer equipment room at SunGard Availability Systems Limited restricted to authorised individuals only.</p> <p>Sandyford office server and network equipment is located in secure server rooms accessed by fob key wherever office space allows.</p>	<p>The server room located at SunGard Availability Systems Limited has hardware devices to protect against power outages and fluctuations. There are also a number of environmental devices to ensure the upkeep and monitoring of the equipment contained within the server room.</p> <p>Uninterruptible Power Supplies (UPS Systems) are installed to ensure against short term power outages.</p> <p>The server room is equipped with raised floors, temperature controls and fire/smoke detectors. Alerts are sent to IT Operations if thresholds are breached and a daily email is sent to members of IT of the environment status.</p>	<p>Reviewed the SunGard service to ensure physical access is restricted and protected. Inspected the Sandyford fob register to ensure restricted access to the Sandyford server room. Ensured UPS systems are in place and monitored.</p> <p><b>No relevant exceptions noted.</b></p>

	<b>Information Technology</b>	<b>Objective</b> Development and implementation of new systems, applications and software, and changes to existing systems, applications and software, are authorised, tested, approved and implemented	
	<b>Process</b>	<b>Control</b>	<b>Result of Accounting Testing</b>
7.19	Application system software changes are approved prior to work commencing. Changes are submitted via a change control system and appropriate testing is conducted (including functional and User Acceptance Testing) prior to authorising the changes to be made to the live environment.	Application system software changes are approved by members of the Board prior to work commencing. Changes are submitted via a change control system. The testing of changes (including functional and User Acceptance Testing) is conducted prior to authorising the changes.	For a selection of changes made during the period on the applications, determined whether they had been authorised and had been tested (both functional testing and User Acceptance testing where applicable) prior to deployment to the live environment. <b>No relevant exceptions noted</b>
	<b>Information Technology</b>	<b>Objective</b> Data migration or modification is authorised, tested and, once performed, reconciled back to the source data.	
	<b>Process</b>	<b>Control</b>	<b>Result of Accounting Testing</b>
7.20	Direct access to change/modify business data (e.g. super- user/ database administrator access) is controlled. End users may only make changes to the underlying data base and master files via the front-end applications	Direct access to business data is restricted to SQL Programmers and Sys Admin.	Inspected access permissions for users with direct access to business data and noted that this was restricted to SQL Programmers and Sys Admin users. <b>No relevant exceptions noted.</b>
7.21	Changes to underlying data are only made on receipt of an approved request.	Requests are authorised by an appropriate business user/data owner.	For a selection of data changes made, noted that each data change was approved by an appropriate business user / data owner. <b>No relevant exceptions noted.</b>

<b>Information Technology</b>		<b>Objective</b>	
<b>Process</b>		<b>Control</b>	<b>Result of Accounting Testing</b>
7.22	Our servers and data are continuously replicated from our Sandyford existing Hyper-V infrastructure to the Microsoft Azure Site Recovery DRaaS.	This is real time replication of our data and systems.	Inspected the Microsoft agreement to confirm real time replication.
<b>Information Technology</b>		<b>Objective</b>	
<b>Process</b>		<b>Control</b>	<b>Result of Accounting Testing</b>
7.23	There is a dedicated IS Help-desk that logs and resolves user issues related to IT hardware and software. Issues are tracked and those that cannot be immediately resolved are escalated within the Information System function accordingly.	The IS Helpdesk monitor and log any incidents of hardware failure reported and resolve at the earliest opportunity.	Obtained and inspected the helpdesk log to ensure timely resolution of IT issues. No relevant exceptions noted.
<b>Information Technology</b>		<b>Objective</b>	
<b>Process</b>		<b>Control</b>	<b>Result of Accounting Testing</b>
7.24	Recovery plans which provide for the recovery of all key business processes are in place.  Recovery plans exist and are maintained to cover the applications and systems which support all business processes carried out at each location.	The Business Continuity Plan is reviewed annually.	Obtained and reviewed evidence of the review of the BCP and of its annual testing.  <b>No relevant exceptions noted.</b>
7.25	Formal documented agreements are in place with outsourcing providers to cover the service offering including physical security, data security and SLAs.	A "Managed Services Agreement" is in place between APT and SunGard in respect of the hosted services. The agreement is reviewed at least annually by IT. Any changes noted will require approval from the Board.	Obtained and reviewed evidence of the annual review and Board approval. No relevant exceptions noted.

7.26	Outsourcing providers carry out performance and capacity monitoring for hosted services and there are regular service reviews.	Real-time performance monitoring is carried out by SunGard and any breaches are immediately logged	Obtained and reviewed evidence of real time monitors and the breaches log. <b>No relevant exceptions noted</b>
<b>8</b>	<b>Insurance Cover</b>	<b>Objective</b> <b>Suitable and up to date insurance cover is maintained.</b>	
	<b>Process</b>	<b>Control</b>	<b>Result of Accounting Testing</b>
8.1	A full programme of insurance is maintained with a range of underwriters as advised by the company's brokers. Cover includes errors and omissions, fidelity and employer liability. Insurance is reviewed annually prior to renewal date to ensure cover is adequate and up-to- date	Insurance renewals are reviewed by the Group Executive.	Through observation and enquiry, inspected the insurance certificates for evidence of review by the Group Executive.  <b>No relevant exceptions noted.</b>
<b>9</b>	<b>Building Security</b>	<b>Objective</b> <b>Suitable and up to date insurance cover is maintained.</b>	
	<b>Process</b>	<b>Control</b>	<b>Result of Accounting Testing</b>
	Access to the APT offices by employees is controlled.	Employee access is by swipe card, which must be carried at all times.	Through observation and enquiry, evidenced, that the access to the building was controlled by swipe cards. <b>No relevant exceptions noted.</b>
	Access to the building and car park is controlled by swipes and fob cards.	Access is overseen by building security personnel	Through observation and enquiry, evidenced, that the access to the building was controlled by swipe cards. <b>No relevant exceptions noted.</b>

# An Award-Winning Team



**WINNER**  
Communication Award



**WINNER**  
Pensions Technology Award



**WINNER**  
Excellence in DC Award



**WINNER**  
Innovation Award