Appendix

Review of Internal Controls at Investment Managers

Aviva Investors

"Report on Internal Controls" for the period 1 October 2016 to 30 September 2017.

Auditors: PricewaterhouseCoopers LLP

Basis of Qualified Opinion (Page 14)
As stated in the management statement by Aviva Investors in section B, evidence of the effective operation of controls to ensure that client portfolios are monitored for compliance with investment limits, guidelines and restrictions for the subset of rules subject to manual monitoring or self-certification could not be provided. We are therefore unable to conclude that the following control objectives were achieved for the period 1 October 2016 to 30 September 2017:

i. Section 1. Investment Management (Objective 1.5.1) - Client portfolios are managed in accordance with investment objectives, monitored for compliance with investment limits and restrictions and performance is measured
ii. Section 2. Indirect Property Management (Objective 2.5.1) - Client portfolios are managed in accordance with investment objectives, monitored for compliance with investment guidelines and restrictions and performance is measured

Opinion (Page 14)

In the auditor's opinion, in all material respects, except for the matters described in the Basis for Qualified Opinion paragraph:

a) the description in sections D to G fairly presents the Service Organisation's and the included Subservice Organisation's investment management services for institutional clients and pooled funds and information technology as designed and implemented throughout the period from 1 October 2016 to 30 September 2017;

b) the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls operated effectively throughout the period from 1 October 2016 to 30 September 2017 and customers applied the complementary user entity controls referred to in the scope paragraph of this assurance report; and

c) the controls tested which, together with the complementary user entity controls referred to in the scope paragraph of this assurance report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 October 2016 to 30 September 2017.

Of the 228 controls tested by the auditor, 11 exceptions were identified.

These exceptions and the management responses are included at the end of this appendix.

BlackRock

"Report on Controls at BlackRock Placed in Operation and Tests of Operating Effectiveness for Asset Management Services" for the period October 1, 2016 to September 30, 2017.

Auditors: Deloitte and Touche LLP

In the auditor's opinion, in all material respects:

a.) The description fairly presents the System that was designed and implemented throughout the period October 1, 2016 to September 30, 2017.

b.) The controls related to the control objectives stated in the Description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2016 to September 30, 2017, and subservice organizations and user entities applied the complementary controls assumed in the design of BlackRock's controls throughout the period October 1, 2016 to September 30, 2017

c.) The controls operated effectively to provide reasonable assurance that the control objectives stated in the Description were achieved, throughout the period October 1, 2016 to September 30, 2017 if complementary subservice organization controls and complementary user entity controls assumed in the design of BlackRock Service Organization's controls operated effectively throughout the period October 1, 2016 to September 30, 2017.

Of the 140 controls tested by the auditor, 4 exceptions were identified:

1) **Page 102 – Control P.1.2** – For the GLM job scheduler, a configuration change was made which resulted in the potential for unauthorized users to access the internal job scheduling tool. Upon identification, management updated the configuration to restrict access to authorized employees. In addition, inappropriate GLM processing occurring as a result of unauthorized changes would be identified through reconciliation controls tested at M.1.4, M.2.2, M.2.3, M.3.1 and M.3.2.

   Management Response: Management updated the GLM job scheduler configuration to restrict access to authorized employees. Additionally, management confirmed that unauthorized changes to batch job schedules would be identified as a result of Securities Lending operational control activities which rely upon batch processing in the GLM application

2) **Page 105 – Q.1.3** – For 2 of 71 individuals across transfers and terminations selected for testing, noted the transfer notification was not sent timely

   Management Response: Management has re-emphasized the importance of accurate notification for modification of access for transferred employees in accordance with policy. Additionally, management noted that one of the two late notifications identified was the result of a data feed error between the HR system of record and downstream corporate groups. Management performed a review and confirmed that this data feed issue was an isolated event, and has implemented an exception report to identify any similar issues that may occur in the future.

3) **Page 106 – Q.1.6** – For 2 of 45 transfers selected for testing, noted the user access was not updated on a timely basis per BlackRock policy.

Management Response: Management has re-emphasized the importance of timely modification of access for transferred employees in accordance with policy.

4) **Page 107 – Q.1.10** – For 1 of 45 servers and databases selected for testing, D&T noted 7 of 234 users with administrative access whose access was no longer authorized. Upon investigation, noted these 7 users did not log in past the date where access was no longer authorized.

   Management Response: Management has confirmed that these 7 accounts had previously been deactivated, and access was reinstated due to a software bug with a disaster recovery failover process which was limited to one in-scope database. Exposure checks were performed to confirm that no activity was undertaken as part of reinstatement, and process improvements have been taken to avoid similar instances in the future. In addition, periodic recertifications are in place to ensure that database access is reviewed and updated according to policy; this issue arose in between recertifications.

GMO

"Report On GMO's Description of its Advisory Services System and on the Suitability of the Design and Operating Effectiveness of Controls" for the period October 1, 2016 to September 30, 2017

Auditors: PricewaterhouseCoopers LLP

In the auditor's opinion, in all material respects:

a.) the description fairly presents the Advisory Services System that was designed and implemented throughout the period October 1 2016 to September 30 2017;

b.) the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1 2016 to September 30 2017 and user entities applied the complementary controls assumed in the design of GMO's controls throughout the period October 1 2016 to September 30 2017;

c.) the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period October 1, 2016 to September 30, 2017 if complementary user entity controls assumed in the design of GMO's controls operated effectively throughout the period October 1, 2016 to September 30, 2017.

Of the 126 controls tested by the auditor, 0 exceptions were identified

However, the following controls although 'No exceptions' noted, could not be tested

Page 69 – Control 3j – Reason: During the period, there were no instances of updates to the purchase and redemption fee tables within GPRS; therefore the operating effectiveness of this control could not be tested.

Page 100 – **Control 12g** – Reason: There were no GMO Australia Separately Managed Accounts during the period; therefore the operating effectiveness of this control activity could not be tested for GMO Australia Separately Managed Accounts.

Page 101 – **Control 12h** – Reason: There were no GMO Australia Separately Managed Accounts during the period; therefore the operating effectiveness of this control activity could not be tested for GMO Australia Separately Managed Accounts.

Oldfield Partners LLP

"AAF 01/06 Assurance Report on Internal Controls" for the period 1 July 2016 to 30 June 2017

Auditors: Deloitte LLP

In the auditor's opinion, in all material respects:

a.) the description on pages 11 to 42 fairly presents the control procedures of Oldfield Partners LLP's investment management services that were designed and implemented throughout the period 1 July 2016 to 30 June 2017;

b.) the controls related to the control objectives stated in the description on pages 11 to 42 were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls operated effectively throughout the period 1 July 2016 to 30 June 2017; and

c.) the controls that we tested were operating with sufficient effectiveness to provide reasonable assurance, that the related control objectives stated in the description were achieved throughout the period 1 July 2016 to 30 June 2017.

Of the 151 controls tested by the auditor, 1 exception and 1 Limitation of Testing was identified

1) **Page 35 – Control 7.2.7** – Passwords to access Eze OMS and Eze Compliance via Citrix (Gateway) did not expire between the period 10/09/2016 – 30/06/2017 due to the password expiry setting had been disabled as part of the data migration of the Eze server.

2) **Page 36 – Control 7.2.9** – Limitation of Testing – The audit log for Third parties accessing OP's server is retained only for 7 days. As such testing was limited to 7 days in the audit period.

Pantheon

"Type II Report on Controls Placed in Operation Relating to Investment Advisory and Management Activities" for the period from 1 October, 2016 to 30 September, 2017

Auditors: KPMG LLP

In the auditor's opinion, in all material respects:

a.) the Description fairly presents the Investment Advisory and Management Activities system as designed and implemented throughout the period from 1 October 2016 to 30 September 2017;

b.) the controls related to the control objectives stated in the Description were suitably designed throughout the period from 1 October 2016 to 30 September 2017; and

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 from 1 October 2016 to 30 September 2017.

Of the 109 control objectives tested by the auditor, 0 exceptions and 1 Limitation of testing was identified:

1) Page 55 – Control MF20 – Limitation of Scope: KPMG enquired of management whether any instance of an authorised signatory partner not being available occurred during the period and were informed that no instances had occurred. Since there were no instances, the operating effectiveness of the control could not be tested.

Record Currency Management Ltd

"Report on Internal Controls (AAF 01/06)" for the period 1 April, 2016 to 31 March, 2017.

Auditors: Grant Thornton UK LLP

The auditors confirmed that in all material aspects:

a.) the accompanying report by the directors describes fairly the control procedures that relate to the control objectives referred to above which were in place as at 31 March 2017;

b.) the control procedures described on pages 11 to 71 were suitably designed such that there is reasonable, but not absolute, assurance that the specified control objectives would have been achieved if the described control procedures were complied with satisfactorily,

c.) the control procedures that were tested, as set out in the body of this report, were operating with sufficient effectiveness for us to obtain reasonable, but not absolute, assurance that the related control objectives were achieved in the period 1 April 2016 to 31 March 2017.

Of the 150 controls tested by the auditor, 0 exceptions were identified.

Standard Life Investments

"Internal Controls Report" for 1 October 2016 to 30 September 2017

Auditors: KPMG LLP

In the Auditor's opinion, in all material respects:

a.) the description on pages 22 to 108 fairly presents the internal controls that were designed and implemented throughout the period from 1 October 2016 to 30 September 2017;

b.) the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls operated effectively throughout the period from 1 October 2016 to 30 September 2017 and;

c.) the controls that we tested were operating with sufficient effectiveness to provide reasonable assurance that the related control objectives stated in the description were achieved throughout the period from 1 October 2016 to 30 September 2017.

Of the 282 controls tested by the auditor, 6 exceptions were identified:

These exceptions and the management responses are included at the end of this appendix.

State Street Global Advisors

"SOC 1 – System and Organization Controls (SOC) for Service Organizations" July 1, 2016 – June 30, 2017

Auditors: Ernst & Young LLP

In the auditor's opinion, in all material respects:

a.) the Description fairly presents the System that was designed and implemented throughout the period July 1, 2016 to June 30, 2017;

b.) the controls related to the control objectives were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period July 1, 2016 to June 30,2017 and if State Street's Information Technology and Global Security divisions and user entities applied the complementary controls assumed in the design of SSGA's controls throughout the period July 1, 2016 to June 30, 2017;

c.) the controls operated effectively to provide reasonable assurance that the control objectives were achieved throughout the period July 1, 2016 to June 30, 2017 if State Street's Information Technology and Global Security divisions' controls and complementary user entity controls assumed in the design of SSGA's controls operated effectively throughout the period July 1, 2016 to June 30, 2017.

Of the 157 controls tested by the auditor, 2 exceptions were identified:

1) **Section IV Page 21 Control 12.8** – For 1 of the 4 months selected for testing, 2 out of 19 variances reviewed did not have evidence of research and resolution. For 1 of the 4 months selected for testing (including 65 invoices with 1 variance), there was no evidence of secondary Finance Associate review.

   Management Response: Management acknowledges that for 2 out of the 19 variances reviewed in the monthly reconciliation, evidence of research and resolution was not provided. In addition, for 1 of the 4 months selected, there was no evidence of secondary Finance review. Management further notes that the invoices were correct and approved (refer to control 12.7 for the approval control). Management has reinforced with appropriate personnel the requirement to document evidence of review.

2) **Section IV Page 22 Control 12.11 –** For 8 out of 35 manually accrued fees selected for testing, the review by the Accounting Manager did not identify incorrect fee calculations.

   Management Response: Upon detailed review, management identified that:

For 2 of 35 investment management fees selected for testing, the review did not identify incorrect invoice calculations regarding fee rate change in the middle of the calculation period. Management has subsequently implemented an enhanced checklist to document the secondary finance reviews of new fee schedules and amendments. Standardized fee schedule language and an exception review process for non-standard fee arrangements is currently being implemented to ensure accuracy for complex arrangements.

For 6 of 35 management fee accruals, management did not identify incorrect fee accruals which resulted from inaccurate spreadsheet formulas. Management has also implemented enhanced spreadsheet controls including documentation of a secondary recalculation of new or revised accruals and checklist signoff by the accounting manager

Aviva Investors (Page 94 – 97)

SECTION H: MANAGEMENT RESPONSES TO EXCEPTIONS NOTED

Control Reference	Control Description	Test of Control Procedures and exceptions noted
1.2.7.2	The Global Responsible Investments team conducts a secondary review of ISS (voting platform) for votes that are over 3% of total holdings to ensure that proxy voting instructions are generated, recorded and carried out accurately and in a timely manner.	**Reliance on Controls Assurance team** For a sample of votes where the vote represents more than 3% of all votes being cast, inspected evidence that the votes were subject to a secondary review prior to the vote. **Exception noted** For 2 out of 26 proxy vote issues (where votes were over 3% of all votes being cast) sampled, secondary review by the Global Responsible Investments team samples was not performed prior to the vote deadline.
Management Response	The exception identified was caused by a change in resources available to support the control. However in both cases there was no financial impact as voting was carried out correctly. We have now addressed the resources involved in vote operations and will implement an additional check of all meetings subject to the control.	
1.3.2.7	The Valuation Oversight team reviews the daily liquidity fund prices received from BNYM to investigate and escalate instances where: a) the NAV per share does not round to 1; b) daily movement is over 0.10% for the funds that do not have a daily price of 1.00; or c) daily yield has changed by more than 1%, and ensures data within daily yield file ties to daily price files to ensure investments are valued using correct prices.	For a sample of days and funds, inspected liquidity fund review performed by Valuation Oversight for evidence of review and research of items outside tolerance thresholds. **Exception noted:** For 8 out of 60 liquidity funds and days, the Valuation Oversight team review of liquidity fund prices was incomplete.
Management Response	Gaps identified have been remediated. All share classes are now unhidden on the daily monitoring file regardless of whether they are invested in or not. The price file template tabs have also been protected to ensure any new class launches will be highlighted and included in the check.	
1.3.2.9	The Asset Pricing team raise all internally valued assets that breach pre-defined thresholds for month-on-month price movements to the AIGPVC on a monthly basis to ensure accuracy of price movements and valuation of assets.	For a sample of internally valued assets that breach the agreed thresholds/tolerances inspected evidence to confirm that they were investigated and commentary was provided to the AIGPVC. **Exception noted:** For 1 out of 5 months sampled, all internally valued assets that breached predefined month on month price movement thresholds were not reviewed by the AIGPVC.
Management Response	We note that in the November pack 2 models had price movements over the 2% threshold which were not reflected in the pack, and 3 models were in the pack but were not highlighted as having movements above the 2% threshold. This exception has been fully remediated and we have noted no issues with subsequently tested samples. The month-on-month price movements for internally valued assets was reviewed by the Pricing team and the Fund Managers for November 2016. The AIGPVC monitors pricing activities (errors, near misses, models), including review of proposed amendments to the pricing policy if required through the monthly AIGPVC meeting and action log to ensure that pricing activities are in line with the approved pricing policy. The 2% movement threshold is only a small part of that discussion. The Management Information packs are appropriately detailed, for example the month-on-month activity for the total value for internally modelled assets for the current and preceding 4 months is reviewed. The MI Appendix section in each pack is further devoted to information on the models.	
1.5.1.4	The Mandate Monitoring team manually monitors investment guideline restrictions (which cannot be coded as automated rules) through review of trade data and sign off on an at least quarterly basis to ensure compliance with investment limits and restrictions.	For a sample of manually monitored guidelines and periods, inspected the Mandate Monitoring team's working papers for evidence of review and that potential breaches were researched. **Exception noted** For the period 1 October 2016 to 30 September 2017, there were 10 investment rules impacting 6 different funds where effective manual monitoring could not be evidenced to ensure compliance with investment limits and restrictions.

Control Reference	Control Description	Test of Control Procedures and exceptions noted
Management Response	Within the instances, 2 funds containing 6 of the investment rules had no transactions in the period. The remaining 4 funds only had 15 transactions in the period. The Mandate Monitoring team recognise the reasons for the occurrence of the above and have introduced additional oversight over delegated monitoring and confirmed there were no further fund reclassifications which had contributed to the above instances. The Mandate Monitoring team have retrospectively checked and confirmed that in the above instances no investment guidelines have been breached. For context, the full extent of rules impacted represent a very small percentage of the total instances of rules. Self-certified and manually monitored rules are typically low risk, many relate to illiquid investments and are unlikely to breach due to the enhanced due diligence and governance at the point of trade. No breaches of self-certified rules have occurred, and only a very few manually monitored rules breaches have occurred, since their introduction in 2014.	
1.5.1.5	The Mandate Monitoring team obtains self-certification confirmations from fund managers for rules or restrictions that cannot be monitored independently, on an annual basis to confirm that they are in compliance with investment limits and restrictions.	For a sample of self-certified guidelines, inspected the self-certification checklists or emails for evidence that self-certifications were performed in a timely manner. **Exception noted** For the period 1 October 2016 to 30 September 2017, there were 29 investment rules impacting 3 different funds which missed a self-certification to ensure compliance with investment limits and restrictions.
Management response	The Mandate Monitoring team have conducted a full review and have identified no other instances of failure to receive a self certification. The Mandate Monitoring team have retrospectively checked and confirmed that in the above instances no investment guidelines have been breached. For context, the full extent of rules impacted represent a very small percentage of the total instances of rules. Self-certified and manually monitored rules are typically low risk many relate to illiquid investments and are unlikely to breach due to the enhanced due diligence and governance at the point of trade. No breaches of self-certified rules have occurred, and only a very few manually monitored rules breaches have occurred, since their introduction in 2014.	
4.1.1.3	1 October 2016 - 1 February 2017: IT users The Access Control Team receives a notification of a leaver via the Workday tool. The leaver's physical access card is then manually set to disable by the Access Control Team on the Granta system on the specified leave date to ensure access is terminated in a timely manner. 1 February 2017 onwards: IT Users The Access Control Team receives a notification of a leaver via the Workday tool. The leaver's physical access card is then manually set to disable by the Access Control Team on the SecureNet system on the specified leave date to ensure access is terminated in a timely manner. For 3rd party access it is the line manager's responsibility to notify the Access Control Team within 7 days when there is a leaver. The 3rd party leaver's physical access card is then manually set to disable by the Access Control Team on the SecureNet system to ensure access is terminated in a timely manner.	**Reliance on Controls Assurance team** For a sample of terminated employees in the period, inspected evidence that each individual's physical access card had been disabled on the specified leave date. **Exception noted** For 7 out of 45 access cards sampled, timely removal of access cards to the Aviva Investors building could not be evidenced on the Granta system.

Control Reference	Control Description	Test of Control Procedures and exceptions noted
Management response	The Granta system was decommissioned when Aviva Investors moved out of the Poultry building on 1 February 2017. The required evidence from the Granta system was not retained and therefore we have been unable to evidence the date at which access cards to the Poultry building were disabled/removed. At Aviva Investors' new building, St Helens, no exceptions relating to non-timely access removal were identified.	
4.1.1.4	**1 February 2017:** The Granta system is configured to disable physical access passes that have not been used for 30 days. Annually, Facilities management conduct a review of the Granta system user access list to ensure passes that have not been used in over 100 days have been disabled. **1 February 2017 onwards:** The Access Control Team run a SQL query upon SecureNet to obtain a list of all cards that have not been used for more than 30 days on a weekly basis. This list is then reviewed and cards not used for 40 days and still active are then manually disabled.	**Reliance on Controls Assurance team** **Granta** - Inspected evidence that the Granta system has been configured to automatically disable physical access passes which have not been used for 30 days. For the full population of physical access passes that had not been used for 30 or more days, inspected evidence in the Granta system that these had been automatically disabled. **SecureNet** - For the full population of physical access passes that had not been used for 40 or more days, inspected evidence in the SecureNet system that these had been manually disabled. **Exception noted** Poultry Building - For the period 1 October 2016 to 1 February 2017, it was not possible to obtain evidence of the automated job on Granta system to disable cards that had not been used within 30 days. St Helens Building - For the period 1 February 2017 to 10 May 2017, it was not possible to demonstrate the effective operation of the control as a list of all cards that had not been used for more than 30 days was not retained.
Management response	The Granta system was decommissioned when Aviva Investors moved out of the Poultry building on 01 February 2017. The required evidence from the Granta system was not retained and therefore we have been unable to demonstrate the auto disabling of access cards to the Poultry building. At Aviva Investors' new building, St Helens, from 01 October 2017 access cards have been auto disabled on the new system after 30 days of inactivity and no exceptions were identified.	
4.1.2.2	**1 October 2016 - 12 June 2017** IT Security Administration and where applicable, application support teams are responsible for the creation of access in line with the approved request. This ensures access granted is appropriate, a separate designated requestor and approver raise and approve new account requests before the access is created for both standard and privileged accounts within Teamworks or Assyst. **12 June 2017 onwards** IT Security Administration and where applicable, application support teams are responsible for the creation of access in line with the approved request. This ensures access granted is appropriate, a separate designated requestor and approver raise new account requests before the access is created for both standard and privileged accounts within IT Care or Assyst. **Windows:** The IT Security Administration Team creates a standard network account when a new joiner alert is raised in Workday by People Faction Services. Any additional access required will then follow the process outlined above. Note: For the Aladdin application 3rd party BRS set up the application account on receipt of an approved request.	**Reliance on Controls Assurance team** For a sample of new standard and privileged accounts created in the period, inspected that access requests had been granted after approval by the designated approver within Teamworks. **Exception noted** For 2 out of 45 new access samples, evidence of approval prior to the access being granted could not be obtained.
Management response	Retrospective approval for access requests and the historic approval from the line managers prior to the team member joining has been obtained for the sample selected. Evidence being unavailable due to system limitations will no longer recur (as the Teamworks system has been decommissioned).	

Control Reference	Control Description	Test of Control Procedures and exceptions noted
4.1.2.3	**1 October 2016 - 12 June 2017** IT Security Administration is notified of the leaver request via an automated email and set the Windows AD account to expire within 24 hours of the specified leave date. IT Security Administration or the application support team revoke application access within 30 days post the specified leave date depending on the authentication mechanism in place for each application. Note: For the Aladdin application 3rd party BRS remove the application account on receipt of an approved request from IT Security Administration. **12 June 2017 onwards** The same process was followed but Teamworks was replaced by Workday.	**Reliance on Controls Assurance team** Inspected evidence that leavers' access to the Windows AD network had been revoked within 24 hours of the specified leave date and that access to the applications had been revoked 30 days post the specified leave date. **Exception noted** For 2 out of 208 leavers, access to the network was not revoked at the time of testing. Additionally, for 6 out of 45 accounts sampled, it was not possible to evidence network revocation within 24 hours of the specified leave date.
Management response	Identified gaps have now been remediated. No leaver accessed any system post their leave date. The Teamworks tool was decommissioned in June and evidence of access removal for the 6 network accounts was not retained. Evidence being unavailable due to system limitations will no longer recur (as the Teamworks system has been decommissioned). The existing monthly control to detect inactive Active Directory accounts (4.1.2.9) is now included in the AAF report from 19 May 2017 which reviews inactivity of 30 days to aid in identifying potential leavers. A detective control is now in place whereby when leaver notifications are received after the leaver's leave date the appropriate investigation is performed to check the leaver has not accessed any system since leaving. It is our aim to bring this check into the 2018 AAF report control activity.	
4.1.2.6	The estate management team reviews an automated Splunk report that details out laptops that do not have the appropriate Safeguard encryption package on a daily basis with Assyst tickets being raised automatically to resolve issues to ensure the Safeguard encryption package is applied on all laptops. Note: Refer to 4.4.2.2 for details of the incident management controls to evidence the timely resolution of Assyst tickets raised.	**Reliance on Controls Assurance team** For a sample of days in the period, inspected evidence that the automated Splunk report showing laptops without the Safeguard encryption package had been generated and reviewed, and that Assyst tickets were raised to resolve issues. **Exception noted** For 3 out of 45 laptops identified without the Safeguard encryption package, Assyst tickets had not been raised to resolve the issue or the tickets remain unresolved.
Management response	The laptops identified in the sample have now been encrypted.The raising of the Assyst ticket is now fully automated which has streamlined the process and will prevent any further errors from occurring.	
4.3.1.4	Segregation of Duties exist between Release Management team and deployment team. **SAMS** SAMS follows the common release management process. In addition to this the DMZ server deploys changes into production which is restricted to the AIGBD team. DXC manage access to the DMZ server as part of the third party support agreement.	**Reliance on Controls Assurance team** Inspected evidence that approved changes from the Serena Dimensions tool to a pre-deployment folder were deployed by the Release Management team. Inspected evidence that write access to the folder was restricted to authorised members of staff who were not developers. Further inspected evidence that access to the folders where changes were stored in the production environment was restricted to the Environment Management and Delivery teams responsible for moving the changes into the production environment. **Exception noted** One user account was identified with inappropriate write access to the pre-deployment folder.
Management response	Incorrect access was inadvertantly given and the user account was immediately removed during testing. The user cannot deploy code into production with this access and there is adequate segregation of duties between those who can add code into the pre-deployment folder and those who can deploy code into production.	

Standard Life (Page 109 – 113)

The service Auditor's tests have identified six exceptions. Responses from management in respect of exceptions noted by the Service Auditor in performing testing of Standard Life Investments Limited controls are presented below to provide additional information to users of this report.

1.	Descriptions of Controls	Service Auditor's Tests specific to the exceptions noted
6.9	On a daily basis, a reconciliation is performed by the Derivative Trade Support team over the accuracy of the OTC trade data between CRIMS, the OTC Database and Citi data. Any differences noted are investigated and resolved as appropriate by an independent individual.	**Inspection** For a selection of days, inspected evidence that the reconciliation of data between the OTC Database, CRIMS and Citi was performed by the Derivative Trade Support team and that any differences were investigated and resolved by an independent individual. ***Exception noted*** For one out of 15 items tested, evidence was not seen of the investigation and resolution of differences being performed by an independent individual, through completion of the daily checklist.
Management response		
Management can confirm that the reconciliation differences were investigated and closed appropriately, with management approval of the closures at the time evidenced within a request to the Technology Support team to close the breaks on management's behalf. The paper checklist was not completed to retain the evidence for the task being completed in the usual fashion. Management now sign off the checklist on a weekly basis to ensure completeness.		

2. Descriptions of Controls	Service Auditor's Tests specific to the exceptions noted
10.2 With the exception of North America, active voting decisions of proxy voting instructions are appropriately analysed (with the exception of de minimis holdings). Proxy votes are signed by an authorised person (as per the ESG Investment Voting Authorities) within the Company and instructed on the voting platform. All auto votes (smaller holdings), with the exception of de minimis holdings, with policy recommendations to vote against management are reviewed and authorised (as per the ESG Investment Voting Authorities) before being released from the ISS Proxy Exchange voting platform.	**Inspections** For a selection of proxy vote meetings during the period and regarding proxy votes above the de minimis holdings and outwith North America, inspected evidence that votes were analysed and signed-off by an authorised person as per the ESG Investment Voting Authorities. For the same selection, inspected evidence that any auto votes which were voted against management recommendations were reviewed and authorised as per the ESG Investment Voting Authorities, before being released from the ISS voting platform. ***Exception noted*** The full population of 12 proxy vote meetings was tested. For seven out of the 12 meetings, evidence was not seen that auto votes which were voted against managment recommendations had been analysed and signed off by an authorised person.

Management response

Management can confirm that this was due to a coding issue in relation to a report which we receive from our proxy voting provider. Management can also confirm that the report has since been corrected and notifies the team of any meetings that are coming up to be voted where we have a small holding and a recommendation to vote against management. All meetings sampled were voted in line with policy.

Two new checks have also been implemented within the process:

(a) a daily check of any Votes Against Management identified on the proxy voting provider's platform; and (b) an addition to the Daily Vote Check report, identifying holdings above de minimis with an against recommendation going through as an auto vote. In addition, a quarterly review of these particular auto votes takes place.

3. Descriptions of Controls	Service Auditor's Tests specific to the exceptions noted
12.6 1 Oct 2016 to 22 May 2017 On a daily basis, the Valuation & Pricing Oversight (VPO) and Derivative Control teams receive a 3 way OTC derivatives valuation reconciliation from BNYM (between MarkIT or Superderivatives, the counterparty and Bloomberg AIM). The reconciliation is reviewed for positions which are outwith predefined tolerances by the Derivatives Control team. Sign off is provided to VPO to either confirm BNYM values are reasonable or highlight prices for BNYM to investigate and provide further support for. VPO instruct the NAV release only once any investigations have reached an acceptable conclusion.	1 Oct 2016 to 22 May 2017 **Inspection** For a selection of days during the period, inspected evidence that the OTC reconciliations were reviewed for positions which were outwith predefined vendor tolerances and sign-off provided to VPO prior to authorising NAV release. ***Exception noted*** For one out of 10 days selected, evidence was not seen of sign-off being provided to VPO prior to authorising NAV release.

Management response

Management can confirm that, in relation to the exception, verbal confirmation was received from the Derivatives Control team at the time that the derivative valuations were accurate. Management can also confirm the accuracy of the NAV which was released, and note that this control no longer operates.

4. Descriptions of Controls		Service Auditor's Tests specific to the exceptions noted
4.4	A permitted level of due diligence expenses and/or abort costs is detailed in the PIR and approved by the relevant Investment Committee. Expenses in advance of a PIR may be incurred with the prior written approval of SL Capital's CIO.	**Inspection** For a selection of potential investments during the period, inspected evidence that the level of due diligence expenses permitted had been detailed within the PIR and that this was approved by the relevant Investment Committee. ***Exception Noted*** For one out of eight items tested, evidence was not seen of a permitted level of tax due diligence expenses detailed in the PIR and approved by the relevant Investment Committee.

Management response

Tax due diligence is a normal part of the due diligence undertaken on all co-investments. Due to the accelerated deal completion time frame in this particular case, the tax engagement was not formally approved by the Investment Committee, but was verbally approved between the Chief Investment Officer and the deal team. The overall due diligence costs for this transaction were consistent with the nature and quantum of due diligence on similar investments. The investment procedures around formal documentation/ governance of due diligence costs have been reviewed and have been re-emphasised to the deal teams.

5. Descriptions of Controls		Service Auditor's Tests specific to the exceptions noted
7.3	Cash transaction reports detailing the previous day's transactions are produced and reviewed by the Finance Analyst team on a daily basis to ensure complete, accurate and timely settlement of payments and receipts. Outstanding cash transactions are monitored and reviewed on a weekly basis to ensure timely settlement of outstanding payments and receipts.	**Inspection** For a selection of days, inspected evidence that the daily cash transaction report was produced and reviewed by the Finance Analyst team to ensure complete, accurate and timely settlement of payments and receipts. For a selection of weeks, inspected the outstanding cash transactions report for evidence that the cash position was reviewed and settlement of outstanding payments and receipts was monitored. ***Exception Noted*** For one out of five weekly outstanding cash transactions reports selected, evidence of a review of the prepared report was not seen.

Management response

Management can confirm that the report in question was accurately prepared and that, as part of this preparation, all outstanding investment transactions were investigated with no further action deemed necessary.

Management can also confirm that cash flows are monitored on a daily basis by both SL Capital Partners and the respective fund administrator to ensure that any outstanding payments or receipts are identified immediately and resolved in a timely manner, and therefore the risk associated with this exception is deemed immaterial.

6.	Descriptions of Controls	Service Auditor's Tests specific to the exceptions noted
2.5	Users' permission level access for key applications is reviewed for appropriateness on an annual basis by line managers. Any inappropriate access is removed on a timely basis.	**Inspections** Inspected results of the annual user access permission level review and determined that users' permission level access for key applications is reviewed on an annual basis by their line manager. For a selection of users identified as having inappropriate access as part of the annual review, inspected evidence that the users' permission level access for key applications had been removed on a timely basis. ***Exception Noted*** For four of the 25 selected users, the access was not removed on a timely basis.

Management response

Management have added an extra step into the recertification process to ensure that Access Management follow up regularly by e-mail/telephone with the other access teams to receive confirmation that access has been removed in a timely manner.

Table showing number of controls tested by each manager and the number of exceptions as reported to Committee in 2016, 2017 and 2018

Fund Manager	Control Objectives Tested	Number of Exceptions	Control Objectives Tested	Number of Exceptions	Control Objectives Tested	Number of Exceptions
	2016 Report	2016 Report	2017 Report	2017 Report	2018 Report	2018 Report
Aviva	171	8	262	7	228	11
BlackRock	137	4	140	5	140	4
GMO	159	2	147	1	126	0
Insight	133	5	109	1	n/a	n/a
Longview	92	0	106	2	n/a	n/a
Oldfields	153	0	154	1	151	1
Pantheon	107	0	112	1	109	0
Record	137	0	146	1	150	0
Standard Life	334	7	326	11	282	6
State Street	165	4	160	3	157	2