

## Fund Manager and Custodian Results where Control Reports supplied

## Appendix A

<b>Alliance Bernstein</b>		
<b>Auditor:</b> PricewaterhouseCoopers		<b>Period Tested:</b> 01/10/09 to 30/09/10
<b>Control</b>	<b>Test Results</b>	<b>Fund Manager Response</b>
Controls provide reasonable assurance that trade orders are authorised, allocated and recorded accurately, completely and in a timely manner	For two of 55 new securities (equity and fixed income) selected in Melbourne, peer review of security characteristics set-up in APEX could not be evidenced.	The security set-ups were verified as having been done correctly but the paperwork could not be located. Supplemental staff training on the importance of keeping complete records was undertaken
Controls provide reasonable assurance that trading activities are in compliance with client directives.	There is no evidence that access to Error Tracking System was reviewed during the period under review.	Management conducted a formal review of access during October 2010 and removed inappropriate access for two individuals.
Controls provide reasonable assurance that securities are valued using prices obtained from authorized sources in accordance with Alliance Bernstein policy and procedures and are updated into the accounting and reporting systems on a timely basis.	There is no evidence that the access recertification was performed during the year for a shared drive containing pricing spreadsheets.	Management validated that Business user access to the shared drive was appropriate and that the Information Technology personnel had an appropriate segregation of duties based on their shared drive access.
	Two Best Pricing shared folders did not have restricted IT access via break glass nor were the permissions to the folders reviewed on a quarterly basis for appropriateness.	Management has reinforced the requirement to implement a regular access review for these two shared folders.
	One of 22 AB Advantage users was not removed timely after the user no longer required access.	The AB Advantage user, whose access was not removed on a timely basis, was the former manager of the group and had been asked to work on a special project for which access to AB Advantage was approved and required. At the conclusion of the project in late September, access was not immediately removed but has since been removed.

	<p>For two of 47 securities sampled an incorrect price was manually calculated. The two securities were a total return swap and derivative.</p>	<p>The price variance review serves as the compensating control</p>
	<p>For one of 125 manually input security prices, the security price was incorrectly input into Best Pricing.</p>	<p>The price variance review serves as the compensating control.</p>
	<p>For one of 12 months selected, there is no evidence of secondary review of the Derivatives Pricing Checklist.</p>	<p>The remaining 11 monthly control occurrences were reviewed and evidence of secondary review of the derivatives checklist was present. Management has reinforced the importance of properly documenting evidence of the secondary reviews.</p>
<p>Controls provide reasonable assurance that new applications and changes to existing applications are authorized, tested, approved and implemented.</p>	<p>Of a population of 24 administrative IDs/groups with access to the TFS version control system in the first quarter of 2010, one was found with inappropriate access.</p>	<p>The group in question had automatically been installed when TFS was implemented. However, the group in question contains GETS Windows administrators; they are not developers. Hence, separation of duties between the developers who use the product and those with administrative privileges was still maintained. Also, TFS does not contain production business data. Inappropriate access for these individuals would have been restricted to code located on a development server, which would require testing before being promoted to production</p>
	<p>Of a population of 31 administrative IDs/groups with access to the version control system in the third quarter of 2010, one was found with Inappropriate access.</p>	<p>The user's access to the system was appropriate; only the level of access was incorrect due to a CAAG oversight. The access level was rectified post audit.</p>

Controls provide reasonable assurance that logical access to programs and data is limited to authorized individuals.	The ACEBOSSPROD Sybase database does not require passwords to contain at least one alpha character and one numeric character.	The ACEBOSSPROD finding was rectified post-audit. All other password controls were in place; only the "check for digit" option was not working properly.
Controls provide reasonable assurance that production jobs are accurately scheduled and any problems or deviations are identified and resolved	For three of 45 Service-now tickets selected no documented evidence was available to indicate the Service-now ticket was resolved and closed in a timely manner.	The jobs ran successfully at the next scheduled time. Policies and procedures concerning Service-now documentation will be reinforced with technical personnel
Impact on the pension fund	<p>There was no impact for the Hillingdon fund.</p> <p>After each report Alliance Bernstein do an internal review to retroactively ensure there has been no impact to the client. If there was an impact or a failed control objective, there would have been a notification to any impacted client. After each report Alliance Bernstein do post-mortem reviews with the Investment Operations, IT teams and PwC to address lessons learned, exceptions and future plans that may impact IT and Operations controls in scope for SAS 70.</p>	

<b>Goldman Sachs Asset Management</b>		
<b>Auditor:</b> PricewaterhouseCoopers	<b>Period Tested:</b> 01/10/09 to 30/09/10	
<b>Control</b>	<b>Test Results</b>	<b>Fund Manager Response</b>
Controls provide reasonable assurance that client account transactions and cash and security positions are completely and accurately recorded and settled in a timely manner	1 of 25 manually input trades selected for testing were not reviewed by a second individual	Management agreed with observation. In May 2010 control changed to an online review of all trades whereby a second individual (approver) must comment on each individual manual trade.
<b>Impact on the pension fund</b>	<p>To the best of GSAM's knowledge, the exception noted in GSAM's 2010 SAS70 report did not negatively impact the portfolio and remedial actions were implemented.</p> <p>In May 2010, this control was changed to an online review and evidence of this review is available centrally and provides enhanced visibility for management to ensure that 100 % of checks are complete.</p>	

<b>Northern Trust</b>		
<b>Auditor:</b> KPMG		<b>Period Tested:</b> 01/10/09 to 30/09/10
<b>Control</b>	<b>Test Results</b>	<b>Fund Manager Response</b>
Controls provide reasonable assurance that transactions are received from authorised sources	9 of 384 transactions selected were not authorised by personnel on the authorised signers listing.	Management conducted team meetings to train and reinforce various procedures and processes surrounding client transactions.
	7 of 247 transactions tested a call back was not performed. 4 of 247 transactions tested a call back was performed but not in line with procedures.	Updated policy has been approved which provides more clarity regarding requirements. Current implementation efforts include review and update to specific processes, authorities and applicability.
Controls provide reasonable assurance that transactions are completed and accurately recorded in a timely manner	8 of 189 accounts tested 2 had incorrect coding for investment responsibility and 6 had incorrect coding for proxy voting.	A new account set up system is in the process of being implemented which will allow for a more rule- based logic to reduce the opportunity for inappropriate coding
Controls provide reasonable assurance that cash is monitored for overdrawn account balances and uninvested balances are identified and invested in authorised instruments	2 of 112 accounts tested the short term investment vehicle was not appropriately hard coded in the system	Management reiterated with all staff the need for proper coding.  In addition a new account set up system is in the process of being implemented which will allow for a more rule- based logic to reduce the opportunity for inappropriate coding. Additional key field will be reviewed following initial entry
Controls provide reasonable assurance that new assets and changes to assets are authorised and established in a complete, accurate and timely manner on the Trust system	1 of 103 asset setups selected a secondary review was not performed.	Management reiterated the importance of an independent review and that it was required in all instances

<p>Controls provide reasonable assurance that complete and accurate information is obtained from accounting systems to perform specific performance measurement (rate of return) calculations and that adjustments to transaction information are made through appropriate procedures.</p>	<p>5 of 43 clients selected late reporting was not properly tracked for timeliness of completion and delivery</p>	<p>Management will continue to monitor deliverable metrics and provide guidance to staff on the codes they can use to track the timeliness of performance reporting. Additionally management will reiterate to all staff the existing procedures.</p>
<p>Controls provide reasonable assurance that Investment Guidelines are accurately set up/maintained within the NT compliance analysis system and exception reports are properly generated</p>	<p>1 of 24 compliance monitoring subscribers tested the service agreement on file did not match the level of service provided to the client</p>	<p>In this instance the level of service being received was higher than that stated in the agreement.</p> <p>Management is working with Risk Management to establish a practice of imaging SLA documentation as an overall Custody/Legal agreements client have with NT.</p>
<p>Controls provide reasonable assurance that benefit payment transactions are properly authorised</p>	<p>Not applicable to LBH</p>	
<p>Controls provide reasonable assurance that operating system installation, changes and maintenance are authorised, tested and documented</p>	<p>1 of 29 emergency changes did not evidence timely approval within the required time frame of 5 business days.</p>	<p>Although not approved within the required timeframe the change was deemed warranted and ultimately approved by the appropriate manager</p>

<p>Controls provide reasonable assurance that logical access to application data files and programs is limited to properly authorised individuals.</p>	<p>1 of the 37 user selected did not have sensitive access removed upon their transfer</p>	<p>Upon identification management immediately removed access. The user did not create transactions or perform approvals from the date of transfer. Manual business unit reconciliations exist to monitor the integrity of key application data.</p>
	<p>1 of 10 Windows servers had individuals with unnecessary or inappropriate logical access to critical system files.</p>	<p>Upon identification management immediately removed the unnecessary access. No inappropriate access had been used. Management to create a monthly review process that will periodically validate group membership.</p>
	<p>2 of 42 critical application resources selected there were 5 individual ID's that were granted unnecessary or inappropriate access to critical application resources.</p>	<p>Upon identification management immediately removed the unnecessary access. It did not appear that inappropriate access had been used.  Management to implement a weekly review process to help identify and ensure that administrative support access to the application is warranted.</p>
	<p>1 of 35 access violation reports, documentation showing follow up action was taken could not be obtained.</p>	<p>Management determined that the violation related to invalid log in attempts due to incorrect password entry and no unauthorised access was identified. Management will reiterate to staff the importance of documenting follow up action taken</p>
<p>Controls provide reasonable assurance that the NT computer network is adequately secured and monitored to allow permitted traffic, protect against inappropriate intrusions and help ensure transmissions are complete, accurate and authorised.</p>	<p>2 of 10 Windows servers selected a patch update was not installed. Although the primary patch was applied other related sub patches were not included.</p>	<p>Upon identification the sub patches were updated immediately. The risk was mitigated as both servers resided behind the firewall and intrusion detection servers.</p>

<p>Controls provide reasonable assurance that physical access to computer equipment, storage media and program documentation is limited to properly authorised individuals. Preventive and detective controls exist to protect the data centre from environmental hazards.</p>	<p>1 of 6 data centres selected a sufficient periodic access review was not performed. The access list reviewed failed to identify all users with access to the data centre.</p>	<p>The report used was deemed incomplete; however no inappropriate access was identified. Management has enhanced the reporting used to review data centre access going forward.</p>
<p><b>Impact on the pension fund</b></p>		<p>Northern Trust can confirm that London Borough of Hillingdon was not impacted by any of the exceptions noted in the SAS70. None of the exceptions highlighted in the report required new procedures or systems to be set up that were relevant to London Borough of Hillingdon.</p>

## **M&G (State Street Corporation as custodian and fund administrator)**

M&G do not produce an internal control report, however their fund administrator's and custodians State Street Corporation do. The custodian has legal title to the fund's assets and has a regulatory obligation for ensuring that the fund is operating within set guidelines. In these instances the fund manager does not handle client money.

<b>Auditor: Ernst &amp; Young</b>		<b>Period Tested: 01/11/09 to 31/10/10</b>
<b>Control</b>	<b>Test Results</b>	<b>Fund Manager Response</b>
Controls provide reasonable assurance that portfolio investments and cash balances are completely and accurately stated and cash availability is reported accurately and timely.	For 1 of 40 daily cash reconciliations selected evidence could not be found the reconciliation had been performed	Although no same day reconciliation evidence could be provided the activity was reviewed for the respective days and it was confirmed all discrepancies were researched and resolved.  Management has reiterated the importance of maintaining necessary support evidencing review and approval.
Controls provide reasonable assurance that logical access to production applications, databases and operating systems is restricted to authorised individuals based on business need.	1 of 18 access requests for application access the documentation for the request and approval were not available.	Management acknowledges documentation was not available. The user was a member of the development team and members of the team require read only access to perform their job.  Management has reiterated that access will not be granted to members of the development team without an approved access request form.
	2 of 25 terminated users selected, notification of termination was not sent to the security administration personnel in a timely manner.	Management acknowledges notifications was not sent in a timely manner, however once received access was promptly removed.  Management has implemented an automated notification process to prevent this from reoccurring.

	2 of 25 user ID's selected for testing access to production applications was restricted to State Street personnel based on job description.	Management acknowledges that the access for two read only users was not timely removed. Management will implement a process with the business teams to notify the security administration team monthly of all transfers and terminations to ensure the timely removal of access.
Controls provide reasonable assurance that changes to production applications, databases and operating systems are tested, approved and reviewed prior to implementation.	For 18 vendor recommended operating system patches selected, 2 of 18 administration personnel did not approve the change prior to implementation and 1 of 18 system administration approval was provided after the change implementation date	Management acknowledges evidence of prior approval could not be provided, however considers these exceptions to be a result of a documentation issue as these were authorised changes that were required to be installed.  Management has reinforced change control procedures for documenting and retaining approvals with systems administration personnel.
<b>Impact on the pension fund</b>	State Street does not disclose whether a specific client's fund was impacted under the review. M&G and their auditor will review the exceptions that would be applicable to them and determine how significant they deem them to be, and then decide if further audit of client specific procedures was required to gain assurance. On this occasion the auditor of M&G did not believe the exceptions to be significant and so did not investigate further.	

<b>Marathon</b>		
<b>Auditor:</b> Deloitte	<b>Period Tested:</b> 01/01/10 to 31/12/10	
<b>Control</b>	<b>Test Results</b>	<b>Fund Manager Response</b>
Transactions are undertaken with only approved counterparties.	2 brokers with active status on the order management system were not on the compliance approved broker list.	Whilst no trades were executed with either counterparty, it is important that we ensure that all brokers in the OMS mirror those detailed on the Approved Broker List. In order to ensure this remains so, we completed a one-off exercise to purge any old broker details from the system and going forward the Head of Compliance, who manages changes to the Approved Broker List, will also ensure that all additions and deletions are accurately recorded in thinkFolio.
Investment related and cash transactions are completely and accurately recorded and communicated for settlement in a timely manner	1 of 15 new security set up forms could not be located	We firmly believe this to have been an isolated human error and do not envisage making any procedural changes. We have undertaken additional checks and no other forms have been found to be missing.
Proxy voting instructions are generated, recorded and carried out accurately and in a timely manner	1 of 25 proxy votes tested was found to be cast incorrectly.	The cause of the exception was human error when inputting the response into the proxy voting administration system. We have strengthened the controls surrounding this manual process by ensuring that all votes cast are reviewed by another member of the Proxy Voting team before being confirmed in the system.
<b>Impact on the pension fund</b>	There was no impact on the Hillingdon portfolio as a result of these exceptions.	

SSgA		
Auditor: Ernst & Young		Period Tested: 01/07/09 to 30/06/10
Control	Test Results	Fund Manager Response
Controls provide reasonable assurance that client contribution and redemption activity is authorised and recorded accurately, completely and timely	1 of 140 letters tested did not contain evidence that the verification of trade authorisation was performed	Management acknowledged that one letter did not contain evidence of a call back. SSgA subsequently confirmed the instruction was valid. Management have communicated and reinforced the importance of evidencing call backs consistent with their guidelines.
(A firecall ID is an administrative account (systems and infrastructure) that lies disabled the majority of the time. If a situation arises where an individual needs to, in case of emergency or escalation, make use of this special access, they can call a dedicated admin group and have it temporarily enabled to correct a problem or troubleshoot an issue on the particular system it gives control over.)	2 of 50 ID requests selected for testing, appropriate IT Manager approval to authorise activation could not be provided.  1 of 7 Firecall ID approvers/designees selected for testing evidence for recertification could not be provided	While management recognises approval could not be provided in the two instances, the Firecall ID was approved but used beyond the specified time parameter. The technology supporting the application has since been updated preventing use beyond the specified time parameter. Management have confirmed the use of the ID was for legitimate business purposes.  Management has reviewed controls and procedures to strengthen the workflow related to granting to Firecall approval. In addition the process has been fully integrated and is now included in the overall Firecall recertification procedure.
Impact on the pension fund	SSgA are unable to say if the London Borough of Hillingdon were included in any of the samples chosen, however as the examination centres on controls, any exceptions highlighted would be reviewed and suitable remedial action(s) implemented.	

<b>UBS</b>		
<b>Auditor:</b> Ernst & Young		<b>Period Tested:</b> 01/01/10 to 31/12/10
<b>Control</b>	<b>Test Results</b>	<b>Fund Manager Response</b>
Controls provide reasonable assurance that reporting of client account and investment data is complete and accurate.	<p>For the period January 2010 to June 2010, for five out of eleven samples selected, E&amp;Y observed that dual sign off on a spreadsheet was used to evidence four-eye review. Due to the absence of access or lock down controls, we do not consider the spreadsheet control to be designed effectively.</p>	<p>Upon receipt of E&amp;Y's notification, for those five instances where dual sign off on a spreadsheet was used to evidence four-eye review, an additional review was undertaken of the returns calculated and included in client reports by the Head of Performance, UK. All returns were found to be correct. UBS can confirm that the use of quality checklists to evidence four-eye review is in place and being adhered to.</p>
Controls provide reasonable assurance that logical access to databases, data files, programs, and operating systems are reasonably restricted to properly authorised individuals	<p>1 user from a sample of 25 new joiners was setup before line manager and application owner approval was provided. In mitigation, the access granted was in line with business requirements.</p> <p>8 movers from a sample of 25 for which access rights that were no longer required had not been removed in a timely manner. In mitigation, these users did not inherit any conflicting access rights.</p> <p>2 new MAP user account creations from a sample for 5 for which line manager and application owner approval could not be verified. In mitigation, the access granted was in line with business requirements</p>	<p>The user set-up and movers issues noted have been achieved retrospectively. Re-training has been performed to re-emphasize use of the strategic user access tool as intended for the Joiner, Mover and Leaver process. Also a project has commenced to automatically remove movers from the application.</p>

	<p>2 users from a sample of 25 leavers were not removed from the Carousel and Cosmos applications, and 1 user that was not removed from the Sophis and GIM II applications in a timely manner. In mitigation, network access for these users had been revoked in a timely manner.</p>	<p>The 3 user access removals relating to application level access have been achieved retrospectively and completed. The primary control relating to network access disallowed the application level access from being used. Re-training has been performed to reemphasise use of the strategic user access tool as intended for the Joiner, Mover &amp; Leaver process and a project has commenced to automatically remove leavers from Global Asset Management applications. As at March 2011 this project is 50% complete with the remaining automation to be completed in October 2011.</p>
	<p>Our review found that a system default group had not been replaced/removed from the databases supporting the Longview, Tradeflow and MAP applications. This is a configuration that does not comply with the UBS secure build standard. In mitigation, users with access to the system default group identified no exceptions.</p>	<p>The system default group access has been removed for the applications in-scope and controls have been implemented to scan UBS databases on a periodic basis to identify any recurrence of the issue. As part the UBS review, they validated that access to the group was restricted to authorised IT personnel.</p>
	<p>The Security Operations Centre (SOC) team responsible for security logging and monitoring activity on platforms does not currently log and alert on key privileged user activity. Specifically, key privileged user activities are not monitored with predefined alerts. In mitigation, privileged user access rights to the operating system and databases supporting the applications in-scope identified no relevant exceptions.</p>	<p>Logging and monitoring over the activities noted across the applications in-scope is now in place. The UBS infrastructure team has also further enhanced controls relating to managing Highly Privileged access as part of the "Infrastructure Privileged Access Control Program." The program includes identification of associates that have Highly Privileged access, implementation of pre-defined alerts for privileged users' activities, periodic review of defined alerts and systematic review of Highly Privileged accounts by senior management.</p>
<b>Impact on the pension fund</b>		Of the exceptions noted there was no detrimental impact on the Hillingdon portfolio.

**Ruffer****Auditor:** Ernst & Young**Period Tested:** 01/10/09 to 30/09/10**Impact on the Fund**

The audit report showed there were no exceptions in relation to the controls tested. There was therefore no impact on the Fund

**Fauchier (HSBC as custodian and fund administrator)**

Fauchier Partners do not produce an internal control report, however their fund administrator's and custodians HSBC do. The custodian has legal title to the fund's assets and has a regulatory obligation for ensuring that the fund is operating within set guidelines. In these instances the fund manager does not handle client money.

**Auditor:** KPMG

**Period Tested:** 01/01/10 to 31/12/10

**Impact on the Fund**

The audit report showed there were no exceptions in relation to the controls tested. There was therefore no impact on the Fund

## Fund Manager Responses where no Control Report Supplied

### Macquarie

Macquarie Infrastructure do not produce a report on internal controls, such as the SAS 70 or AAF 01/06. However, Macquarie claim internal controls are core to the operations of the funds both at a fund level and through their Risk Management Group (RMG).

Risk within Macquarie is owned at the business level with business heads responsible for identifying risks within their businesses and ensuring that they are managed appropriately. Clear controls exist in relation to credit, market, operational, regulatory and reputation risks. These areas have implications outside the businesses and are tightly controlled by the RMG.

The RMG is an independent, central unit responsible for ensuring all risks are appropriately assessed and managed across Macquarie. Its functions are Credit, Prudential, Capital and Markets, Operational Risk and Compliance. The Head of RMG has oversight of Internal Audit jointly with the Board Audit and Compliance Committee (BACC).

Two divisions of the RMG have the greatest impact on the Macquarie infrastructure business. Compliance assesses legal, regulatory and reputation risks from a Macquarie-wide perspective. It creates Macquarie-wide policies and procedures to manage these risks and monitors and oversees the management of compliance risks by each of Macquarie's businesses. Internal Audit provides independent assurance to senior management and the BACC on the adequacy of design and the effectiveness of Macquarie's financial and risk management framework.

Macquarie Infrastructure and Real Assets is responsible for the internal controls impacting their business, with each fund's Chief Operating Officer (COO) playing an important role in ensuring the operations and internal control procedures are adhered to. The COO's and their operations team perform a number of functions including ensuring the fund operations are compliant with constituent documents and Macquarie's policies and procedures.

The Macquarie Finance team are primarily responsible for the implementation of the Macquarie's financial controls. The Macquarie Finance team are part of the Central finance division of Macquarie and not directly part of the Macquarie Funds Group. This gives the Macquarie Finance team independence from the Macquarie Infrastructure and Real Assets division, allowing them to operate with objectivity.

Specialist functions within Macquarie Infrastructure and Real Assets (such as Corporate Communications, Legal, Company Secretarial, Tax etc) are also responsible for the controls environment within their areas of expertise.

### **Private Equity**

Adams Street Partners and LGT Capital Partners have been contracted on a fund of funds basis. As such they are consolidating the accounting of managers to which funds are committed. Both managers have considered the implementation of a SAS 70/AAF 01/06 review but to date have deemed it unnecessary.

All the funds held by the private equity managers have undergone an audit of their financial statements. Although not expressly checking internal controls an audit includes consideration of internal control over financial reporting as a basis for designing audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the internal controls over financial reporting. The full complement of 2010 accounts for private equity is yet to be audited but where available an unqualified opinion was provided. Prior year's accounts have been checked and these show no qualified opinions.