"Your money is safe with us" – investment firms and meeting the burden of proof

If the poet Elizabeth Barrett Browning had been an investment professional surveying the many options she has to address her client's due diligence concerns she may well have started her famous sonnet with the line:

"How do I prove your assets are safe? Let me count the ways"

It is nothing new for firms in the investment industry to need to satisfy current and future clients that they are a safe and secure home for their assets. But this challenge has undergone a recent step change in difficulty as clients seek both higher levels of comfort and more robust forms of evidence. A combination of the Madoff fraud and the collapse of Lehman Bros (and the near collapse of other banks) has driven a huge hole through any sense of complacency that money is safe with an organisation simply by virtue of its reputation and regulated status. We have entered the age of 'trust but verify', but without much 'trust' and with lots of 'verify'.

This challenge applies to organisations up and down the investment value chain, from investment advisors to investment managers on to administrators and custodians. They all share the need to prove they are a fit and proper organisation with whom to deal. Given this is basically an identical need in every organisation, there are an alarming number of different methods by which they can try to achieve it. This paper looks at the different options available and asks whether any one of these approaches might be a silver bullet solution the industry and its clients can accept as a standard.

The table overleaf examines the pro's and con's of the alternatives. These summarise as:

- Options with no fixed structure (individual due diligence and SAS 70's) although often the structure is effectively dictated by the client, with verification by the client in the former case and by an audit firm for the latter.
- Options which do have a fixed structure in so far as they define what the investment firm must be doing to earn a clean report (AAF01/06 and CEFEX). These are purpose designed for the investment industry but by virtue of their prescriptive nature they set quite a high standard (though not an unreasonable one).
- Options which seem to nibble around the subject by virtue of being designed for a different purpose (ISO 9001, Sarbanes-Oxley).

Assuming we dismiss these last, marginal, alternatives, and place a caveat on AAF01/06 as it has little currency outside the UK, the decision narrows to embracing the internationally recognised SAS 70 or the newcomer CEFEX. Both are a desirable alternative to individual due diligence as they provide comfort in one exercise and holding the accreditation can be used to proactively market the firm.

Which is the better alternative? It's a close call. CEFEX compliance probably shows you are a better firm top to bottom and does a good job of addressing more subjective areas such as investment decision making and risk management. By contrast a SAS 70 has much higher recognition value, at least at this point and is tougher (i.e. more audit verification) on hard operational controls. CEFEX is generally a harder standard to reach compliance with, meaning potentially more upfront investment, but the SAS 70 has the higher annual cost of proving ongoing compliance. CEFEX clearly suffers in the comparison from its relative newness and no more than 100 firms currently have it, and those are predominantly in the US. If CEFEX continues to grow in popularity (and many more firms are working towards it) and get more traction outside the US, then it has the potential to be a clear winner versus the SAS 70. Until that time we'll call it a tie.

1. Individual due diligence

What is it:

Client and potential clients have their own staff or representatives conduct interviews and review materials to reach a conclusion.

Pro's	Con's
➢ Only as hard as your clients want to make it.	➢ Only as hard as your clients want to make it. ➢ Logistical and administrative overhead of managing multiple different visits. Disruptive of normal operations. ➢ Nothing tangible to market to potential clients.

2. SAS 70 / ISAE 3402

What is it:

Statement on Auditing Standards No. 70 is the US accounting approach by which 'service organisations' can provide comfort to their clients. International Standard on Assurance Engagements No. 3402 is the international equivalent. Generically they are usually referred to as SAS 70s. These standards dictate how a firm goes about producing a report on itself which their clients (and their auditors) can place reliance on without the need for further work. A SAS 70 report details the key controls present in the firm and an assessment by an auditing firm of how well they are operating.

Pro's	Con's
➢ Scope is flexible, can focus on a few controls or group of assets. ➢ Internationally recognised. ➢ Used as a marketing tool. ➢ Traditional focus on accuracy of reporting and asset security make it more relevant to custodians and administrators.	➢ Clients know the 'flexible scope' can be abused to make the firm look good by excluding problem areas. ➢ Not very good at processes with a lot of judgement (like investment decision making). ➢ Significant (£50k+) one-off cost to prepare. Annual cost (c. £30k?) to get it audited.

3. AAF 01/06

What is it:

Audit Assurance Faculty (of the UK Institute of Chartered Accountants) Technical Release 1 of 2006 was developed for the same purpose as SAS 70's, but is specific to investment firms. It was originally developed to guide pension funds on the type of assurance they should seek from their investment managers. Like a SAS 70 it needs to be assessed by an audit firm (it follows the same audit principles) but, unlike a SAS 70 it prescribes exactly areas of control the investment firm needs to have in place.

Pro's	Con's
➢ Investment firm specific, with variations for different types of firm, from custodians to hedge funds. ➢ Demonstrates a high standard of capability. ➢ Perfect for marketing to pension fund clients.	➢ UK specific so lack of international name recognition. ➢ Comprehensive and prescriptive requirements mean firm may incur significant costs to gain compliance (usually more than a SAS 70).

4. Sarbanes-Oxley

What is it:

The (in)famous Sarbanes-Oxley Act of 2002 was passed into US law in response to the Enron collapse. Mandatory for companies with securities listed in the US there are plenty of international companies who have chosen voluntary compliance. It requires companies to show they have very strong controls over accurate reporting of financial numbers, and requires their auditors to sign this off in the Annual Report.

Pro's	Con's
➢ Widely recognised. ➢ Almost total focus on the accuracy of financial statements is a good fit for investment assets. ➢ Forces the Board of Directors to engage with their controls.	➢ Not common in the investment firm context. ➢ Financial statement focus means not very useful for obtaining comfort on other business processes. ➢ Onerous documentation requirements, therefore resource (and cost) intensive.

5. CEFEX

What is it:

The Certificate of Fiduciary Excellence. Relative newcomer, although based on the Global Fiduciary Standard which has been around for several years. CEFEX is a report of compliance with best practice fiduciary standards. It is audited annually, although the auditors in this case are those who hold the Accredited Investment Fiduciary Analyst certification rather than accountancy firms. The US American Society of Pension Professionals and Actuaries has endorsed CEFEX as the top certification for pension plans to seek from investment firms, but it has mainly been a North American phenomenon to this point.

Pro's	Con's
➢ Comprehensive, covers the quality of management and processes, including subjective areas like investment decision making. ➢ Use as a marketing tool – cache value of being rare / hard to achieve. ➢ Cheaper annual audit cost than a SAS 70.	➢ Reaching a compliant state is not easy, may be costly. ➢ Limited name recognition at this point, limiting value in marketing. ➢ Predominantly US focused to date.

6. ISO 9000

What is it:

The International Organisation for Standardization standard on Quality Management. This standard sets out requirements for managing a process to achieve the quality expectations of clients and has been in existence for decades and implemented by over a million organizations. It requires an annual audit by a firm accredited by ISO, such as the British Standards Institute.

Pro's	Con's
➢ Internationally recognised and used as a marketing tool by the companies who hold it. ➢ Inexpensive annual audit cost.	➢ Rarely applied to investment firms, its generic content is not a natural fit. ➢ Requires lots of process documentation to demonstrate compliance. ➢ The annual audit is relatively 'light touch' which may not be sufficient comfort for all clients.