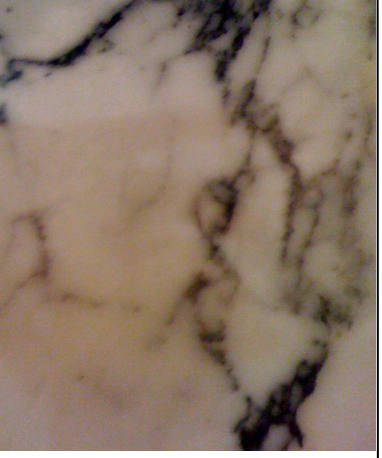

Education Series-
Information Technology Due Diligence

Virtualization. Dark fiber. Load-balancing. Most hedge fund investors may have little idea what these words mean, nor do they think they need to. Many investors may simply raise the question - what do any of the above terms, or similar ones, have to do with the quality, profitability or operational riskiness of a hedge fund manager? The above referenced terms, and a whole other host of seemingly esoteric items, relate to a subject that is often overlooked, and generally minimized, during the operational due diligence process: information technology ("IT"). In the environment of the modern hedge fund, as in most businesses, information technology plays a crucial role. The importance of IT is heightened in knowledge based work environments such as hedge funds. A weak information technology infrastructure and a lack of strategic technology planning can lead to a host of operational inefficiencies which could potentially enlarge any fund losses and reduce overall trading gains. Of note, some key areas investors may want to address during the operational due diligence process include:

Hardware:

- What is the desktop hardware platform in place? Why was this hardware selected? How frequently is it updated?
- What types of servers are utilized? Why did the firm select that server environment?
- How has the firm ensured that data is efficiently backed up and archived? Is redundant hardware in place?

Software:

- What are the primary software applications utilized? Has the firm customized these applications or simply utilize them off the shelf?
- What versions of each of software applications are utilized? Who is responsible for software maintenance? How does the firm determine when software should be updated?
- What recent software initiatives has the firm implemented? What future software projects does the firm anticipate undertaking?
- How do the firm's different systems communicate with each other? How do software systems (i.e. – accounting system) interact with service provider systems (i.e. – administrators accounting system?)

Business Continuity and Disaster Recovery:

- Has the firm customized its business continuity and disaster recovery plans or is a generic plan in place?
- Does the firm perform testing of its plans? How frequently? Is testing performed from just a technology perspective or do employees actively participate in tests as well?
- How long would it take the firm to perform a data restore for system critical functions in the event of a disaster event?

Information Security:

- How does the firm protect proprietary data?
- Are data access logs maintained? Can employees utilize removable media devices?
- Does the firm monitor user profiles? Is penetration testing performed?
- Are IT consultants utilized? If so, how does the firm monitor consultant access to and use of proprietary data?

For More Information

Contact:
Jason Scharfman, Managing Partner
scharfman@corgentum.com
corgentum.com

CORGENTUM

20 Fleet Street, Jersey City, NJ 07306
Tel. 201-360-2430