Operational due diligence has become a hot topic that continues to gain importance and attention throughout the alternative investment industry. Over the past few years, as regulations have changed and investors increasingly seek transparency, funds are spending more time than ever preparing for the due diligence process.

It is no surprise that the investment industry landscape is becoming more and more competitive. As this trend continues, investors are raising their expectations and looking towards funds that display the highest levels in operational excellence. One important way to ensure your firm meets these high standards is to complete a due diligence questionnaire (DDQ) that can be shared with potential investors.

A comprehensive DDQ covers a wide range of topics, from assets under management to audited financial statements and investment strategies. One major area of focus is the fund’s IT and accompanying security policies and procedures. At Eze Castle, we frequently assist our hedge fund clients in completing DDQ questions on technology, and we often see the same types of questions popping up. So, to help you get started, we have compiled the following list of some frequently asked DDQ questions.

**Organization**

1. Provide an organization chart for the Company, its affiliates and key personnel.
2. Provide the physical address and general contact information for each of the Company’s office locations.
3. Provide the name and contact information of the Company employee(s) assigned to the client’s account(s).
4. Provide a list of compliance personnel, their roles and qualifications, the date of his/her appointment and position within the Company’s organizational structure.

**Annual Assessment/Audit**

1. When was the last date on which the Company tested its internal policies and procedures? Please provide a summary of the results.
2. Describe the internal controls that ensure conformity with the Company’s policies and procedures concerning confidentiality of client information.
3. Describe any material violations of the Company’s policies and procedures that relate to the services provided to the client in the last twelve (12) months. If any occurred, please describe the violations and the corrective action that was taken.
4. Describe the Company’s process for (i) reporting violations that directly affect the services provided to the client and (ii) reviewing and assessing the adequacy and effectiveness of its policies and procedures. Please include an explanation of how the Company determines the materiality of violations as well as the process for identifying and reporting violations of policies and procedures internally.
Access Control Policy
1. Does the organization have a formal and well-documented access control policy in place?
2. Is the policy regularly reviewed to determine whether the controls are operating as intended? Are changes and enhancements to the policy implemented when necessary?
3. Does the firm’s IT staff (or technology partner) ensure appropriate access control to applications and sensitive company data? Are there robust procedures in place to grant or deny access to applications?
4. How does the firm manage employee remote access? Are procedures in place to ensure remote access is delivered securely?
5. Has a password policy been implemented throughout the organization? Have all employees been trained on best practices for password security?
6. Are policies in place to force password changes periodically?

Network Security Policy
1. Has the organization developed a formal and well-documented network security policy?
2. Is the policy regularly reviewed to determine whether the controls are operating as intended? Are changes and enhancements to the policy implemented when necessary?
3. Does the firm have a robust firewall in place at the network level? Are policies configured to defend against external security threats? Are the firewall logs monitored regularly?
4. Does the firm employ an intrusion detection system (IDS) to prevent unauthorized access?
5. Is a solution in place to protect email systems against spam?
6. Is a solution in place to ensure mobile devices and laptops are secure in the event of loss or theft? Are email and text messages encrypted and archived?

Physical Security Policy
1. Has the organization developed a formal and well-documented physical security policy?
2. Is the policy regularly reviewed to determine whether the controls are operating as intended? Are changes and enhancements to the policy implemented when necessary?
3. Are access controls in place for the Server Room? How does the firm ensure only authorized personnel gain access critical systems?
4. Are procedures in place to manage visitors in the office? Are steps being taken to ensure visitors do not have the ability to observe or access sensitive employee systems and documents?

Disaster Recovery & Backup
1. Describe the Company’s physical security, disaster recovery and backup plans and procedures.
2. Please describe the communication chain related to the firm’s business continuity/disaster recovery plan.
3. Is the policy regularly reviewed to determine whether the controls are operating as intended? Are changes and enhancements to the policy implemented when necessary?
4. Has the firm tested the BCP from both a technical and operational perspective? How often are these tests performed?
5. Has the firm established a dedicated location to retain backup copies of all critical data?
offsite data encrypted and stored securely?
6. Has a secondary working location been established to which employees should report in the event of a disruption or outage?
7. Do all employees clearly understand the BCP procedures? Have appropriate training and documentation been established and shared with all personnel?
8. Has the firm determined its crucial recovery point objectives (RPOs) and recovery time objectives (RTOs)? Does the DR solution meet these guidelines?
9. Please provide a copy of the Company’s disaster recovery plan.
10. How often is the Company’s disaster recovery plan tested?

**Systems and Information Security**

1. Describe the software system(s) used to provide services to the client, including any relevant security features (e.g., firewalls).
2. Describe any material changes within the past twelve (12) months relating to software systems used to provide services to the client.
3. Where is/are the Company’s data center(s) located?
4. Describe the Company’s security measures with respect to systems access, including who has access (and at what level).
5. Describe in detail (i) what records the Company retains on behalf of the client (in both electronic and physical format), and (ii) for how long the records are kept.
6. Describe the security procedures (e.g., locked filing cabinets) for the protection of physical documents.
7. Describe the Company’s policies and procedures for destroying physical documents.
8. Are ongoing vulnerability assessments performed against the Company’s systems? If so, are the assessments performed by internal personnel or third party service providers?