	Requested Information	YES/NO In Process Partial	Additional Details
1	**Does your organization have a formal Written Information Security Policy? If so,**		
1	**Does your Written Information Security Policy address the following areas: Please provide a copy, or, at a minimum, a screenshot showing the table of**		
1.1.1	*Data Governance and classification policy*		
1.1.2	*Access controls and identity management policy*		
1.1.3	*Configuration management policy*		
1.1.4	*Asset management policy*		
1.1.5	*Risk assessment policy*		
1.1.6	*Data disposal policy*		
1.1.7	*Incident response policy*		
1.1.8	*Systems operations policy*		
1.1.9	*Vulnerability and patch management policy*		
1.1.10	*System, application and network security and monitoring policy*		
1.1.11	*Systems and application development and performance policy*		
1.1.12	*Physical security and environmental controls policy*		
1.1.13	*Data privacy policy*		
1.1.14	*Vendor and third party service provider management policy*		
1.1.15	*Consistent use of multi-factor authentication*		
1.1.16	*Cybersecurity awareness training, which is given to all personnel annually*		
1.1.17	*Encryption to protect sensitive information transmitted and at rest*		
1.2	**Does your Organization have an acceptable use policy that all employees must review and sign off on? If so, please provide a copy or at a minimum, a screenshot/copy of only the table of contents.**		
1.3	**Has the organization aligned their security framework to NIST CSF, CIS, ISO 27001 or equivalent? If yes, please specify.**		
1.4	**Is a background check required for all employees accessing and handling the organization's data or managing the financial assets? If so, what kind of checks are performed?**		
2	**Does your organization conduct Risk Assessments? If so, please answer the following questions**		
2.1	**Are they conducted by a third party, internal, or both. Please specify.**		
2.2	**At what frequency are the Risk Assessments performed? (Annual, semi-annual, etc.).**		
2.3	**Does your Risk Assessment documentation describe how identified cybersecurity risks are evaluated and categorized?**		
2.4	**Does your Risk Assessment document define how existing controls address risks to the confidentiality, integrity, and availability of nonpublic information, and/or the financial assets you manage?**		
2.5	**Does your Risk Assessment program have a procedure to document how risks are either mitigated or accepted?**		
2.6	**Is your Risk Assessment updated to account for changes to information systems, nonpublic information, emerging threats, or business operations?**		
3	**Does your organization have a reliable annual third party Audit of Security Controls?**		
3	**If so, does it encompass the following:**		
3.1.1	*Validation of control design and operating effectiveness*		
3.1.2	*Vulnerability scanning*		
3.1.3	*Internal penetration testing*		
3.1.4	*External penetration testing*		
3.1.5	*Web application penetration testing, if applicable.*		
4	**Does your organization have clearly defined and assigned Information Security roles and responsibilities?**		
4	**If so, does it encompass the following:**		
4.1.1	*Do the persons assigned these roles have sufficient experience and necessary certifications? If so, what certifications?*		
4.1.2	*Does the person in this role maintain current knowledge of changing cybersecurity threats and countermeasures? If so, Please explain how.*		
5	**Does your organization implement strong access control procedures that incorporate the following measures?**		
5.1	**Does your organization limit access privileges (e.g., general user, third party administrators, plan administrators, and IT administrators) based on the role of the individual and adhere to the need-to-access principle?**		
5.2	**Is physical access to data processing equipment (servers and network equipment) restricted? Please explain how.**		
5.3	**Does the organization recertify access to all systems, applications, and data repositories that provide access to Fund data and/or financial assets? If so, what frequency?**		
5.4	**Are employees given local administrator rights to their assigned workstations or laptops?**		
5.5	**Does your organization require all employees to use unique, complex passwords?**		
5.6	**Does your organization utilize multi-factor authentication for all remote access to the internal network and access to cloud based resources, that store, process, transmit, and/or pose a risk to the Fund?**		
5.7	**Does your organization utilize multi-factor authentication to access critical internal servers and network devices.**		
6	**Does your organization have a policy that addresses assets or data stored in a cloud or managed by a third party service provider that are subject to**		
6.1	**Does your organization define minimum cybersecurity practice requirements for third party service providers?**		
6.2	**Does your organization perform a risk assessment of third party service providers as part of the onboarding process?**		
6.3	**Does your organization update their risk assessments of the third party providers on an ongoing basis? If so, please describe.**		
6.4	**Does your organization require third party providers ensure all their subcontractors or processors of Fund data and/or financial assets adhere to the same security requirements set forth with your Organization by the Fund?**		
6.5	**Does the organization require notification per their contracts from their vendors if they are breached and Fund data and/or financial assets are impacted?**		
7	**Does your organization have a formal cybersecurity awareness training program that includes the following:**		
7.1.1	*Training which includes all relevant cybersecurity threats and communication of organization policies?*		
7.1.2	*The training is provided immediately upon hire?*		
7.1.3	*Required to be performed at a minimum of annually thereafter? If alternative frequency, please describe.*		
7.2	**Are Phishing Simulations performed as part of the Cybersecurity awareness training? If so, how often and when was the last one completed?**		
8	**Does your organization have a Secure System Development Life Cycle Program (SDLC)? If so, then**		
8.1	*If your organization develops applications internally, do you have a an SDLC policy?*		
9	**Does your organization have a formalized Incident Response, Business Continuity and Disaster Recovery plan?**		
9.1	**Does your organization have a Business Continuity Plan, which is the written set of procedures an organization follows to recover, resume, and maintain business functions and their underlying processes at acceptable predefined levels following a disruption?**		
9.1.1	*Is the Business Continuity plan tested? If so, how often?*		
9.2	**Does your organization have a Disaster Recovery Plan That provides a documented process to recover and resume an organization's IT infrastructure, business applications, and data services in the event of a major disruption?**		
9.2.1	*Is the Disaster Recovery plan tested? If so, how often?*		
9.3	**Does your organization have an Incident Response Plan That provides a documented process to handle IT incidents which affect business operations?**		
9.3.1	*Is the Incident response plan tested? If so, how often?*		
##	**Does your organization encrypt sensitive data. If so, then…**		
10.1	**Are all workstations, laptops, and end user storage devices encrypted?**		
10.2	**Are server hard drives encrypted? If no, are reasonable physical security controls implemented?**		
10.3	**Is the data encrypted in transit across networks not controlled by the Organization?**		
10.4	**Is a database being utilized to store sensitive information?**		
10.4.1	*Are the tables which is storing that sensitive data encrypted?*		
##	**Does your organization implement strong technical controls implementing Best Security Practices including the following items?**		
11.1	**Does your organization require hardware and firmware models and versions be kept up to date?**		
11.2	**Does your organization require vendor-supported firewalls?**		
11.3	**Does your organization utilize intrusion detection and prevention appliances/tools?**		
11.4	**Does your organization maintain current and regularly updated EDR system?**		
11.5	**Are system and security patches applied to workstations and servers on a routine monthly basis for both operating system and third party applications?**		
11.5.1	*Does your organization monitor for zero day threats or critical vulnerabilities that require a timely response?*		
11.6	**Does your organization perform routine data backup (preferably automated)?**		
11.6.1	*Are the backups stored at a reasonable distance from the source data and is ransomware resilient?*		
11.7	**Does the Organization have SIEM to collect, alert and report audit log events?**		
11.8	**Does your organization have an internal or external 24x7 Security Operations Center (SOC) to monitor and respond to threats?**		
11.9	**Does the Organization support wireless? If so,**		
11.9.1	*How is authentication to the wireless performed? Is there a password shared amongst employees or via network login credentials?*		
11.9.2	*Is guest wireless provided? If so, is it logically or physically separated and access controlled from the private segment?*		
##	**Cyber Insurance and Breach History**		
12.1	**Has the Organization Procured Cybersecurity Insurance? If so, can you please provide us with your "Certificate of Coverage".**		
12.2	**Has the Organization had any Security Breaches in the past 5 Years that impacted Fund data or financial assets? If so, please describe and provide additional details on how the root cause of the breach was addressed and controls corrected or improved.**		

Organization Information	Responses
Organization Name	
Name of POC filling out questionnaire	
Role within Organization	
Email:	
Phone:	
If required - Can the reviewer make contact for clarification or request of additional information? (Yes/No)	
POC if not you for follow up:	
What services does your Organization provide for the Fund?	
What type of Company data do you transmit, process, store or transmit?	
PII	
PHI/ePHI	
Restricted (SSN, Financial Account Numbers, Credit Cards…etc.,)	
Does the Organization have a SOC 1,2 or ISO 27001? If so, please provide a copy.	

Please complete the following worksheets. For each area, please provide as much detail as possible to expedite the review and provide the context necessary. For example, if you answer No, Partial, or In Progress, please let us know the extent of the current state or the relevant completion date. We understand all answers are not a simple yes or no, and context needs to be considered.

For some of the areas, we do ask for evidence. If you are not comfortable sharing any information in that capacity, we are happy to schedule a call so you can either provide more detail or show us on a screen sharing session.

If you have a SOC 1 or 2 Type 2, you do not need to answer every question in this document if it is sufficiently covered in the SOC report, we will review the report to extract the information we need. We only need answers to the questions that would not be covered.

Equally, if you have an alternative vendor due diligence document, such as a SIG or CAIQ, you can provide the document and only answer any questions in this document that are not already covered in what you provided.

If you are a smaller entity with limited staff and resources, please provide as much context as possible regarding the relative risk of the services you provide and controls you have implemented if not to the full extent noted in this questionnaire. Size, risk, and resources will be considered as necessary in overall risk determination and control sufficiency. To further our understanding, we may request a more detailed conversation with you.