BACKSTOP SOLUTIONS®

Every MINUTE matters.®

WHITE PAPER

THIS IS HOW ASSET MANAGERS CAN CONQUER THE SECURITY PORTION OF ALLOCATOR RFIs AND DDQs

EXECUTIVE SUMMARY

Underperformance or a change in portfolio managers are understandable reasons investors might review an investment firm. But according to CoreData Research, investors consider a cyberbreach an even more pressing reason to pursue an investigation. Such investigations can quickly lead to fund managers getting fired. As an asset manager, it is critical that you have a strong cybersecurity program in place and that you are able to communicate the strength of your program to allocators and investors. Here, we provide information on maturing your security posture and offer five guidelines to help you navigate the security section of RFIs and DDQs.

Given this sensitivity to matters involving security, it is crucial for you as an asset manager to have a cybersecurity program in place — and to be able to share the details of that program in a clear and compelling fashion…

As an asset manager, fund performance is your primary concern, but it is certainly not your only concern. You also have to pay close attention to cybersecurity. *Institutional Investor,* in their article "Why Asset Managers Land in the Dog House" quotes a study by CoreData Research that states "institutional investors class a cybersecurity or data breach to be more significant than a fund manager change." In fact, getting hacked is considered sufficient cause by the majority of investors for conducting a special investigation. Given this sensitivity to matters involving security, it is crucial for you as an asset manager to have a cybersecurity program in place — and to be able to share the details of that program in a clear and compelling fashion when responding to requests for information (RFIs) or due diligence questionnaires (DDQs) from allocators and investors.

WHAT IS YOUR SECURITY POSTURE TODAY?

Security can be a challenge, particularly if you do not have a Chief Security Officer (CSO) or Chief Information Security Officer (CISO) to lead the way. If you do not have a security program in place, you need to take action immediately to remedy this lack. One of the best places to begin is with an industry-agnostic security standard such as that provided by the Center for Internet Security (CIS). The CIS Controls™ give you concrete guidance for how to establish solid security for your business. The controls are divided into three categories: Basic, Foundational, and Organizational.

Together, they create “a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks.”

If you do have a security program in place, you should constantly seek to strengthen your security measures. The risk landscape is always changing, hackers are always devising new ways to get inside your walls, and technologies are always improving — for all these reasons, security is about continuing to mature; at no time can an organization say that it has “arrived.”

Not all security measures involve internal controls and processes, however; your vendors and partners play an important role in establishing robust security for your company and your clients. That is why it is important to clearly understand the boundaries of your security program, and to know where you have internal controls in place versus where you are relying on your vendors and partners for security controls. This is crucial because, at the end of the day, you are considered responsible for the security of your investors. You never want to be blindsided by a breach or a regulatory inquiry that reveals a gap in security.

5 GUIDELINES FOR RESPONDING TO SECURITY QUESTIONS ON RFIs OR DDQs

When you respond to an RFI or DDQ, your goal is to present yourself in the best light possible in order to establish a new relationship with a potential investor or fulfill your responsibility to assist with annual due diligence to an existing one. The security section of an RFI or DDQ, however, can be daunting if you are not a security expert. The following five guidelines can help you craft clear and compelling answers that help win new relationships or bolster existing ones.

GUIDELINE #1: BE HONEST AND AVOID EXAGGERATION

It can be tempting to answer “yes” to everything in the security section of an RFI or DDQ in an effort to make a good impression. That inclination should be resisted because it probably does not reflect reality — even if you have a mature security program in place. Rather, you want to provide an accurate accounting of your security measures. Exaggeration (and, of course, outright lying) will open the door to massive liability issues should a breach occur.

GUIDELINE #2: PROVIDE THE BIGGER PICTURE RATHER THAN A YES/NO RESPONSE

Binary questions – that is, questions that require a simple Yes/No response – are a staple of many RFI and DDQ questionnaires. But Yes/No responses fail to provide the bigger picture of how robust your security processes or protocols actually are. If you want an allocator or investor to know the strength of your security measures, you will need to give more than a Yes/No response.

For example, a common binary question is *"Does your firm have an information security policy?"* You could simply answer "Yes," but that does not tell the allocator or investor what your information security policy entails or how it is enforced. It is better to provide a long-form answer or supplemental documentation that describes:

- How access is controlled
- How data is classified
- How cyberthreats are addressed
- How remote access is protected
- How availability is ensured
- How passwords are managed
- How physical security is maintained

Providing the bigger picture will help the investor understand and evaluate your security controls to see if they align with their expectations. It can also serve to differentiate you from a competing fund manager who simply answers Yes/No without additional explanation.

GUIDELINE #3: BE PRECISE WHEN ANSWERING MULTI-PART BINARY QUESTIONS

There is a specific subset of binary questions that is particularly challenging: multi-part binary questions. These are questions that reference multiple items but which only allow for a single response. For example, *"Does your solution provide administrative controls and the capability to provide user permissions based upon group or role, as well as limit the data that can be modified?"* This question references three things: administrative controls, access controls, and data controls. These items are certainly related, but they are not the same. However, questions like these ask you to provide a single answer: Yes or No.

Multi-part binary questions are tough to answer if your security measures do not actually cover every item listed in the question. There are two schools of thought here. Some asset managers will answer "Yes" to

the entire question if they can truthfully say that they do *at least one* of the items mentioned. Other asset managers will only answer "Yes" to such a question if they do all of the items mentioned.

You might think that answering "Yes" is the obvious choice in such a circumstance. But consider: what if the security measure you *don't* have is the one that is *most important* to the investor? That could lead to some very unpleasant results when the investor eventually discovers the lack (as they undoubtedly will).

On the other hand, what if the security measure you don't have is just a "nice to have" and not a "need to have" to the investor or allocator? In that case, answering "No" can cause you to lose out on a mutually-beneficial relationship.

As with the previous guideline, a long-form answer or supplemental documentation is the way to proceed with multi-part binary questions. The investor will appreciate the fact that you have answered with precision, avoiding ambiguity that could cause irreparable damage. When you are precise, you are empowering the investor to make a decision with confidence – and confidence is the foundation for a strong relationship.

GUIDELINE #4: TALK ABOUT CAPABILITIES, NOT TECHNOLOGIES OR TOOLS

Asking about specific security technologies and tools in an RFI or DDQ is common. Investors and allocators often assume that if a certain security technology or tool has garnered a lot of media attention, then it should be a requirement for their asset managers. That is not necessarily true, however, since there can be multiple ways to achieve the same business *outcome* — and it is the outcome that matters.

For example, take the case of data loss prevention, or DLP. DLP is a popular security technology, so many security RFIs contain the question *"Do you have a DLP system implemented?"* Assume for a moment that you do not have a DLP system in place but that you do provide 24/7/365 data monitoring by leveraging other capabilities. You could answer "no" and leave it at that, but in so doing you might lose out on a valuable relationship. Instead, provide a long-form reply or supplemental documentation that demonstrates how you successfully prevent data loss. Discussing the capabilities you have and how they create an equivalent security profile to the technology or tool asked about on the RFI or DDQ enables the allocator or investor to see that you are in alignment with their security requirements.

GUIDELINE #5: BUILD A LIBRARY OF STANDARD RESPONSES AND COLLATERAL

Allocators and investors will typically ask similar questions in their RFIs and DDQs. With that in mind, you can save yourself considerable time and effort by building a library of standard responses so that you do not have to recreate similar language repeatedly. This eliminates the risk of forgetting an important point or making a mistake.

Your library should also include supplemental documentation and collateral that you can provide in addition to the straight RFI/DDQ responses. For example, if you have certifications or audit reports, you can supply those. You can also create data sheets that clearly enumerate your security controls and the benefits they provide. Your vendors or partners may also have documentation about the security measures they have in place. Collateral like this can provide valuable information that the RFI or DDQ may not have asked about directly. It also demonstrates that you place a high priority on security.

QUALITY RESPONSES LEAD TO QUALITY RELATIONSHIPS

The security section of an RFI or DDQ does not need to cause you angst. By following these guidelines, you will be able to respond in a way that is accurate, clear, and compelling. It is true that creating long-form replies and supplemental documentation does require an initial outlay of time and energy. However, as you build a library of responses, you will find that you are able to turn around your response to RFIs and DDQs faster and easier. Additionally, the level of quality detail you provide will open the door to productive conversations with investors and result in long-term relationships.

ABOUT BACKSTOP SOLUTIONS

Because every minute matters, Backstop's mission is to help the institutional investment industry use time to its fullest potential. We develop technology to simplify and streamline otherwise time-consuming tasks and processes, enabling our clients to quickly and easily access, share, and manage the knowledge that's critical to their day-to-day business success. Backstop provides its industry-leading cloud-based productivity suite to investment consultants, pensions, funds of funds, family offices, endowments, foundations, private equity, hedge funds, and real estate investment firms.

CONTACT US

backstopsolutions.com

info@backstopsolutions.com

Main:
+1 312 277-7700

Sales:
+1 312 277-7701

United Kingdom:
+44 0-800-069-8582

Hong Kong:
+852 3511 6015

Chicago (HQ)
233 S. Wacker Dr.
Suite 3960
Chicago, IL 60606

New York
151 W. 25th St.
6th Floor
New York, NY 10001

San Francisco
800 West El Camino Real
Suite 180
Mountain View, CA 94040

Fairfield
2094 185th Street
Suite 1B
Fairfield, IA 52556

London
20 St Dunstans Hill
London
EC3R 8HL
United Kingdom

Hong Kong
7/F, Low Block,
Grand Millennium Plaza
181 Queen's Road
Central, Central,
Hong Kong