BACKSTOP SOLUTIONS®

Every MINUTE matters.®

WHITE PAPER

AN ALLOCATOR'S GUIDE TO ASKING THE RIGHT QUESTIONS ABOUT INFORMATION SECURITY IN AN RFI

EXECUTIVE SUMMARY

Many commonly used security questions in RFIs undercut the due diligence process for institutional investment firms by eliciting potentially misleading, ambiguous, or irrelevant information. Asset Allocators can avoid unnecessary risk in vendor selection by following four guidelines that strengthen and streamline their firm's due diligence activities.

Asset Allocators can avoid unnecessary risk in vendor selection by following four guidelines that strengthen and streamline their firm's due diligence activities.

Security is critical for any organization. But, for the institutional investment industry — dealing as it does with large amounts of money — security takes on a heightened level of importance. Due diligence requires that investment firms include a security section in all requests for information (RFIs) from potential vendors.

Unfortunately, the security questions that are asked frequently have intrinsic weaknesses that undercut an investment firm's ability to adequately evaluate the security profile of a vendor. The result can be serious: an investment firm may choose to partner with a vendor that leaves the door open to unacceptable security risks.

You can strengthen your firm's due diligence activities by asking better, more nuanced security questions that follow four key guidelines. These guidelines can be used to improve your current RFI security section or to vet security questionnaire templates you may wish to adapt for your own use.

GUIDELINE #1: ASK QUESTIONS THAT WILL GIVE YOU THE BIG PICTURE

The goal of an RFI is to gather information that will enable you to make a wise decision about a vendor relationship. Yet, many RFIs are filled with binary questions that do little to further that objective.

A binary question is one that requires a simple Yes/No response from the vendor. They are a staple of many RFI security questionnaires. The problem with binary questions is that they provide you with no data as to the maturity of the security process under review.

Here is a common binary question: "Does your firm have an information security policy?" Assume that a vendor answers "Yes." What does that "yes" actually mean? You still do not know what the information security policy entails or how it is enforced. For instance:

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

A better question to ask is “Explain how your firm addresses information security.” This question will elicit a response that tells you not only if a vendor has an information security policy, but what the policy contains and how well they put information security protocols into practice. You will be able to discern if the vendor has documented processes in place, and evaluate security controls to see if they align with your expectations.

Obviously, it is easier to ask binary questions. It is much simpler to scan an RFI response and tick off how many “yes” and “no” responses a vendor gives. Many investment firms use binary questions because they apply a quantitative scoring approach to their RFI reviews. If there are 50 questions, then a “perfect score” is 50 “yes” answers. The vendor with the highest score is ranked as most desirable.

But binary questions cannot give you a complete picture. For example, imagine that two vendors answer 47 out of 50 binary questions in the affirmative. These two vendors would be considered equal in rank based on their quantitative score. However, what these “yes” responses fail to tell you is that one vendor provides “1-star” and “2-star” quality in those 47 areas, while the other delivers “4-star” and “5-star” levels of security in the same areas. Which vendor would you rather partner with? The one with the more robust security practices. But binary questions will not give you the data necessary to make that distinction, inhibiting you from making the best security and risk decisions for your organization. While it takes more time to review and assess detailed long-form responses, those responses will tell you if a vendor truly has the security in place that your firm requires.

GUIDELINE #2: ASK QUESTIONS THAT AVOID AMBIGUITY

The second guideline also has to do with binary questions, but focuses on a specific subset of them:

Multi-part binary questions. That is, 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, the vendor is asked to provide a single answer: Yes or No.

Multi-part binary questions have all the weaknesses discussed in the first guideline, but add in a new danger: ambiguity. Ambiguity arises because there are two schools of thought among vendors about how to answer such a question if internal security measures do not actually cover every item listed in the question. Some vendors will answer “Yes” to the entire question if they can truthfully say that they do at least one of the items mentioned. Other vendors will only answer “Yes” to such a question if they do all of the items mentioned.

Consider how this plays out in practice. Two vendors are replying to the sample question above. Both vendors have solutions with administrative controls and can provide user permissions based upon group or role, but they each lack the ability to limit the data that can be modified. The first vendor answers the question in the affirmative because they have two out of the three capabilities. The second vendor answers in the negative for the same reason.

This ambiguity has several dangerous ramifications:

- You might assume that the first vendor can do everything that the question lists — but they cannot.
- You might assume that the second vendor has none of the listed controls in place — but they do have some of them.
- You might assume that the first vendor is “better” than the second — but they might be equal as far as this question is concerned.

Such assumptions can open your organization up to significant risk. For example, consider a scenario where an investment firm asks a multi-part binary question that references security capabilities A, B, and C. These capabilities do not carry the same weight, however. Capability A is mission-critical, capability B is important, and capability C is a “nice to have.”

One vendor can deliver on capabilities A and B, but not C. In fact, the vendor is incredibly strong on capability A. However, since they cannot deliver on all three capabilities, they decide to answer the question “No.” The investment firm, having only the “No” to go on, discards the vendor as a candidate, potentially losing out on a strong partner.

Another vendor can deliver on capabilities B and C, but not A. However, since they can deliver on two out of three, they decide to answer the question “Yes.” The investment firm assumes that the “Yes” covers all three capabilities. Only after the vendor relationship is established does the investment firm discover that the mission-critical capability is lacking and that they have to scramble to address an unacceptable level of risk.

In your RFI, be certain to phrase questions in such a way that there is no chance for ambiguity. You need to know that the vendor will interpret the question exactly as you do — otherwise, you will not be able to trust the responses you receive.

GUIDELINE #3: ASK ABOUT CAPABILITIES, NOT TECHNOLOGIES OR TOOLS

Zeroing in on specific security technologies and tools in an RFI is a common yet understandable mistake, especially for investment firms that do not have a security expert on staff. It is natural to assume that if a certain security technology or tool has garnered a lot of media attention, then it should be a vendor requirement. That is not necessarily true.

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?” As already noted, this is a poor question because a “yes” does not guarantee a strong security protocol. After all, Target had a DLP system when they were breached in 2013. The technology was in place but the hackers got in because no one was paying attention to what the system was saying.

A "no" answer to a technology- or tool-oriented question is equally problematic, however, because it might disqualify a vendor who can actually deliver what the investment firm needs. This is true because there are multiple ways to achieve the same result. Using the current example, a DLP system helps secure data, but there are other methods of securing data that do not involve implementing a DLP system. Different technologies and tools can be utilized to deliver an equivalent security profile.

A better way of getting at the information in this case would be to ask "Do you provide 24/7/365 data monitoring? If so, how?" Phrasing the question this way focuses on the desired capability and end result, not on a specific technology or tool. Keep your security goals in mind, and design your RFI questions to allow vendors to tell you how they would deliver against those goals.

GUIDELINE #4: ASK ABOUT WHAT IS IMPORTANT TO YOUR FIRM

Many institutional investment firms do not have security personnel on staff. In that situation, it is common to rely on templates or consultants to provide RFI security questions. Either approach can be very helpful, but there are some pitfalls to be aware of:

- **Questions might be recommended that do not apply to your investment firm.** Asking these questions may introduce confusion into your due diligence process, because you now have to figure out what information you should be looking at from the vendor and what information can be disregarded.
- **Questions might be recommended that you do not understand.** Asking a question such as "What encryption cipher does your organization employ on multi-tenant databases?" when you do not understand encryption ciphers is a waste of the vendor's time and a waste of your time because you will not be able to assess the value of the answer. A better question in this case would be "How are you protecting our data?" which will likely elicit a more understandable response.
- **Questions might be missing about key capabilities.** Templates and consultants provide valuable input, but it is ultimately up to you to know what is critical for your organization and to make sure you ask vendors about those areas.

All of the above bullet points can be summed up very simply: you need to ask about what is important to your firm ... no more, and no less.

DEVELOPING A GREAT SECURITY RFI

As an asset allocator, you want to be sure your due diligence process is rigorous yet targeted. You do not need an exhaustive questionnaire that grills vendors about every last detail of their security profile. Rather, you want to zero in on what is important to your investment firm and phrase questions in such a way that vendors provide relevant information that you can use in making a wise decision. These guidelines will help you do exactly that, strengthening and streamlining your due diligence process.

On the following page, we have provided ten sample security questions that will show you how to craft great questions as well as what to look for in vendors' answers. We welcome you to use these questions with our compliments as you search for vendors to become long-term partners with you in business.

10 SAMPLE RFI SECURITY QUESTIONS

SECURITY QUESTION	WHY THIS MATTERS & WHAT TO LOOK FOR
1. Discuss your administrative controls, including how user access and data access can be governed.	You want to be able to limit access solely to those users whose job functions require it. You also want to limit which users can modify data to only those who require doing so as part of performing their primary job duties.
2. Describe your solution's ability to audit usage by user, including the extent and accessibility of audit trail reports.	Ideally, the system administrator would have the ability to run a report for any user and report on their activity for any given date range. The report should include the date/time of anything accessed or updated within the system, as well as what the actual changes were that were made to data or content.
3. Describe how confidential information is encrypted in transit and at rest.	You want to know how data is encrypted in production, in transit (moving between different systems), and at rest (in storage). You will want to know that they are following industry standards, and if you have specifics that your regulators are looking for, you can ask for these details, but caution: don't get too deep. Cryptography is about complex math algorithms…if you probe too deeply, you may not understand the answers you get back.
4. Does your company conduct regular network and application penetration tests with a third party?	Ideally, the vendor does conduct regular penetration tests through a third party. You want an independent opinion about what your vendor does to enhance their system and protect your data.

SECURITY QUESTION	WHY THIS MATTERS & WHAT TO LOOK FOR
5. Does your company monitor and assess on-going threats for potential risks? If so, how?	You want to make sure your solution vendor is not just performing point-in-time assessments or evaluations, but rather is constantly evolving and improving between those points in time. Ideally, the vendor uses a variety of services and direct monitoring feeds from key sources to stay abreast of the evolving threat landscape (and can provide the names of those services and feeds).
6. Do you have a means by which to monitor your service 24x7 for security-related activities? If so, how?	Threats are 24x7. Criminals don't sleep. The vendor should be able to monitor key systems on a 24x7 basis. They should be able to describe how they achieve this, and with what combination of internal vs. external resources.
7. Do you train your employees/ contractors in security awareness? If so, how?	You want to be sure that all of the people who may come into contact with your sensitive information are diligent and educated about "what could go wrong." The vendor should offer regular security awareness training to all employees and contractors.
8. How are updates rolled out for your application in terms of a) frequency, and b) involvement of our staff?	Security holes can be created when applications and operating systems fall out of alignment. Ideally, the vendor will update their software frequently without requiring intervention from any of your staff (such as with a cloud-based SaaS application).
9. Will we be required to make any networking changes to use your application?	You want to make sure your solution vendor's application does not require some obscure networking rule just to get the application to work. If the vendor utilizes common HTTPS, SSL/TLS security, then you will be able to use the vendor's software solution without making any network changes (assuming you allow standard secure web traffic, such as online shopping).
10. Describe your backup system and if it provides daily copies of critical systems and data?	You want your solution provider to be able to handle everything from a minor business interruption to a catastrophic failure. The ideal response details how data is actively replicated from t he vendor's production site to the vendor's disaster recovery site. Comprehensive responses will also include replication latency settings, tools, how many trailing weeks of data are kept available, how often snapshots are taken, how many days' worth of snapshots are retained, whether storage backups are encrypted, whether they are sent offsite, and how long backups are retained/archived.

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:	Sales:	United Kingdom:	Hong Kong:
+1 312 277-7700	+1 312 277-7701	+44 0-800-069-8582	+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