Mitigating Cybersecurity Threats and Vulnerabilities via Effective Vendor Risk Management Programs

BEST PRACTICE CONSIDERATIONS FOR WEALTH MANAGEMENT INDUSTRY CONSTITUENTS

The intent of this document is to present context required in evolving our cybersecurity due diligence programs, to summarize applicable regulatory requirements, and to outline best practice considerations for performing effective vendor cybersecurity risk management. Simultaneously, this paper highlights cleverDome, Inc., an organization with a vision of collective industry action to solve cybersecurity problems in new and innovative ways.

APRIL 2022

Security Basecamp
(949) 330-0899

Table of Contents

EXECUTIVE SUMMARY

- The independent financial advice industry has experienced significant growth over the past forty years. The associated business models are predicated on openness, choice, and often the integration-on-demand of disparate third-party software solutions in order to serve an independent financial advisor's unique entrepreneurial desire. This model presents notable challenges for information security professionals. This approach often "transfers" the protection of confidential client data outside of regulated financial services organizations into financial services software and services firms (FinTech Vendors) that are not regulated.
- Simultaneously, increased regulatory guidance and enforcement actions in combination with on-going disclosure of cybersecurity breaches at notable FinTech Vendors require stronger management of third- and fourth-party cybersecurity risk. Likely the most challenging aspect of this "mandate" for better third-party cybersecurity risk management is the fact that those expected to do it (e.g. financial advisors), are not necessarily best prepared to perform it.
- According to a study commissioned by eSentire earlier this year, nearly half of firms suffer data breaches at the hands of vendors.[1] Human error and stolen passwords accounted for 26 percent of the breaches, while malware played a key role in many of the attacks. Of the nearly 250 companies that experienced a breach, 32 percent affected personal identifiable data, 29 percent included payment information, and 24 percent exposed proprietary business data. According to the study, only 15 percent of firms reported that their vendor notified them when a breach occurred.
- Given the study's findings, it is important to address the need for a culture of cybersecurity to incentivize human behavior conducive to "judgement based" mistakes. Set your staff up for success. Monitor what processes access personal data and add in redundant controls so that a single human mistake doesn't result in a breach.
- cleverDome, Inc.^{TM} is an Arizona Benefit Corporation (B Corporation) that operates as a Co-Op with Members including FinTech Vendors, custodians, broker/dealers, registered investment advisers, financial advisers and ultimately their investor clients (cleverDome Members). cleverDome has created a community-built model that defines the standards for protecting confidential data and information of consumers in the cloud. cleverDome protects financial services data by taking it "under the Dome", i.e. secure and off the open internet.
- The intent of this document is to primarily outline best practice considerations for performing effective third-party risk management. Various best practices are presented as it relates to gathering vendor attestations, evidencing those attestations, and ultimately making decisions regarding whether a vendor should be approved for use or not.
- Standards are the most foundational element of an effective program. Various standards are outlined in the document, most notably the work performed by cleverDome to galvanize the financial advice industry around what is specifically required by its constituents.
- Many firms do not have the resources required to execute a Third-Party Risk Management (TPRM) program nor the knowledge of how to build such a program. Many firms choose to outsource the function of cybersecurity due diligence to knowledgeable experts that have a defined approach and utilize tools for performing the work.

Essential Points:

- *Regulators have placed significant emphasis on the importance third-party risk management plays in an effective cybersecurity program. FINRA fined Lincoln Financial $650,000 for its failure to supervise third-party vendors in 2016.[2] Simultaneously, vendors must improve processes for handling breaches (e.g. more prompt notification).*
- *Financial Service Industry Regulators, most notably FINRA and the SEC, have actively provided guidance as to improving cybersecurity practices. States, most notably New York and California, have passed laws requiring those they regulate to follow specific cybersecurity requirements. Third-Party Vendor Risk Management is required.*
- *The wealth management industry requires common minimum cybersecurity standards from which to enforce regulatory compliance and information security, and ultimately to prudently protect consumer confidential information. Hackers will grow increasingly sophisticated in exploiting threats and vulnerabilities. A collective approach is essential to combat the continually evolving cybersecurity threats.*

[1] eSentire, "Nearly half of firms suffer data breaches at hands of vendors"; April 2019

[2] Databreaches.net, "FINRA Fines Lincoln Financial Subsidiary $650,000 For Cybersecurity Shortcomings"; November 2016

CYBERSECURITY CHALLENGES FACING THE WEALTH MANAGEMENT INDUSTRY

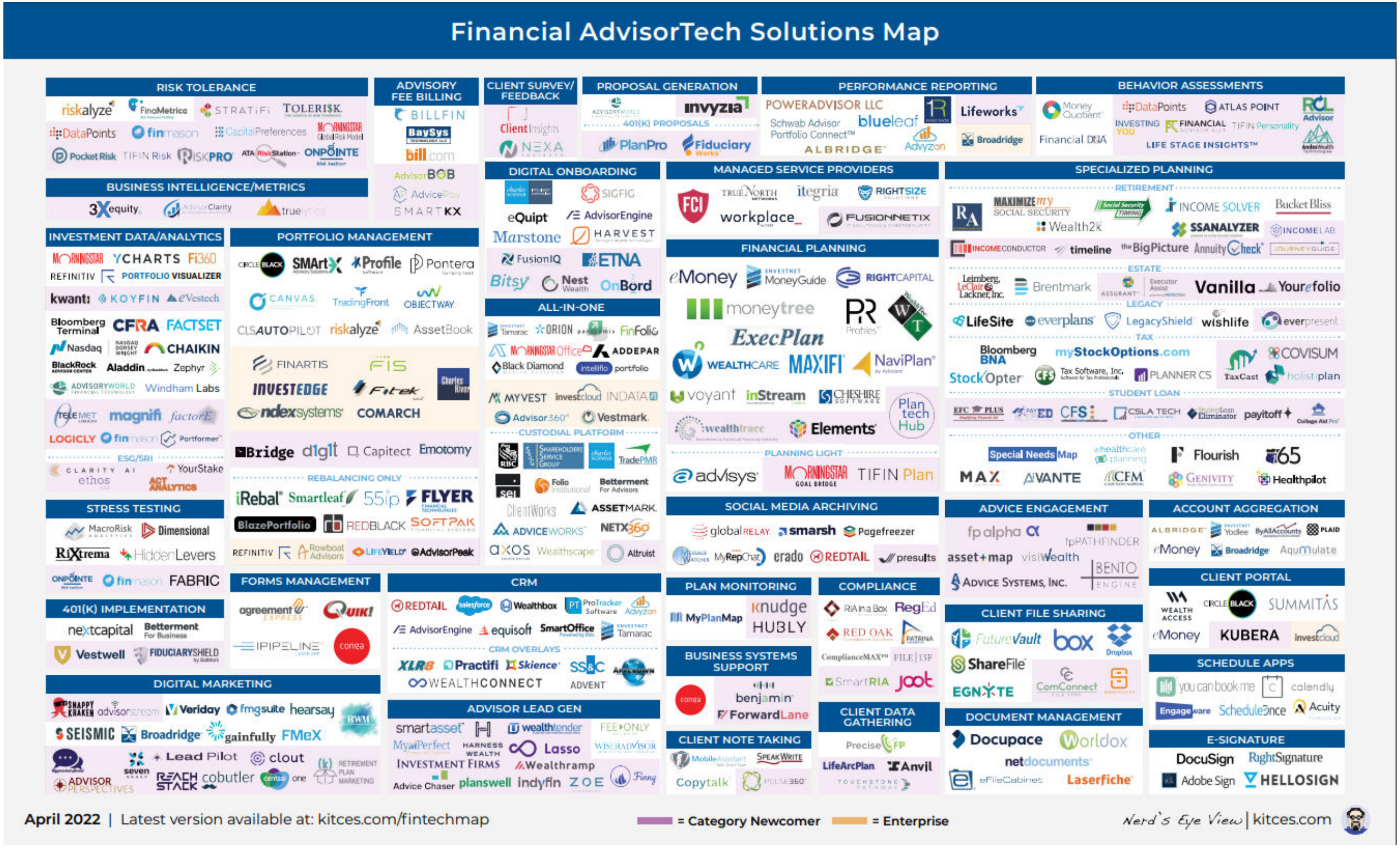
Introduction: An Industry Predicated on the Use and Integration of FinTech Vendors

Over the past thirty to forty years, a combination of factors has contributed to the growth of the wealth management industry. First, enormous growth in investable wealth in the United States combined with greater consumer demand for financial advice. Second, the advent of the internet and the development of the FinTech software niche allowing for "plug and play" solutions strongly desired by financial advisory firms. Many of these advisory firms have set up their own businesses and joined registered investment advisors, and/or aligned with custodians such as Schwab, Fidelity, Pershing, TD Ameritrade and others.

Additionally, many of these financial advisors left large, captive insurance companies, banks, and investments firms to establish their own businesses thereby exercising greater autonomy in terms of how they run their businesses (e.g. hiring staff, establishing business operations, purchasing and integrating technology, etc.). These more "closed organizations", which the advisors left, often offered less choice at least on a relative basis (i.e. a tendency towards fewer products often proprietary, shared operations, shared networks, corporate sponsored or developed technology, etc.) were often easier for information security professionals to secure, but of course information security is not the primary driver of our industry.

Information security now has become the responsibility of the smaller, less centralized organizations (e.g. financial advisors, FinTech software firms, etc.). Industry constituents, notably financial advisory practices, tend to be small to mid-sized, entrepreneurially minded firms. Independent financial advice industry business models are by their very nature predicated on openness, choice, and as referenced above the integration-on-demand of disparate third-party software solutions to serve an independent financial advisor's business needs. The figure below, the Financial Advisor FinTech Solutions Map, was developed and is maintained by Michael Kitces, a well-known expert in our industry. The figure is illustrative of the myriad of choices available to firms and advisors in "assembling" a set of tools to manage their businesses. These tools often store, access, and transmit confidential information of the financial advisors and their clients ("Protected Data") via the open internet.

Figure 1: Financial Advisor FinTech Solutions Map[3]



Business models at firms such as independent broker dealers, investment advisors and the fee only custodians tend to foster the pervasive use (and integration) of cloud-based software solutions depicted above to perform essential business functions (i.e. a bias towards buying and integrating FinTech solutions vs. building custom solutions internally). This often “transfers” the securing of Protected Data “outside” of these regulated financial services organizations – often to relatively small, entrepreneurial FinTech Vendors. This approach presents daunting cybersecurity challenges for its constituents – in particular, for its regulated institutions. Essential Protected Data (and sometimes also the ability to access financial accounts allowing for the movement of money) is often woefully available to anyone from anywhere with an internet connection and a bit of knowledge that is meant to be kept secret.

Simultaneously, increased regulatory guidance and enforcement, in combination with on-going disclosure of cybersecurity breaches at FinTech Vendors, requires stronger management of third- and fourth-party cybersecurity risk. Likely the most challenging aspect of this “mandate” for improved vendor cybersecurity risk management is the fact that those expected to do it, are not necessarily best trained to perform it.

The intent of this document is to present context required in evolving cybersecurity vendor due diligence programs, to summarize applicable regulatory requirements, and to outline best practice considerations for performing effective vendor risk management. Simultaneously, this paper highlights cleverDome, Inc. ™ an organization with a vision of collective industry action to solve cybersecurity problems in new and innovative ways.

Emerging FinTech Vendor Risks

There exists an increasing need for collective action. The relationships between organizations and their FinTech Vendors is at least somewhat complicated. For example, in the event of a breach at one FinTech Vendor that “leaks” data about many broker dealers onto the internet, who is responsible for reporting the breach to the regulators? When should

[3] Kitces.com/fintechmap (web); April 2022

potentially impacted constituents be informed of a breach? Who truly understands the "downstream" implications of how a breach at one FinTech Vendor may impact others? When combating a breach, what actions take place in the first hour, the first day, the next week? Who is responsible and accountable for what?

FinTech Vendors have become prime targets for cyber-attacks. One of the most notable incidents we have seen perpetuated on financial advisors are attacks known as credential stuffing or password spraying. This often involves a threat actor hacking one relatively unprotected FinTech Vendor, lifting advisor usernames and passwords from that FinTech Vendor, and then using those credentials to access other FinTech Vendors used by the same financial advisor. This is done under the assumption that some advisors will simply reuse the same password at more than one FinTech Vendor. We know with certainty based upon numerous cybersecurity incidents managed over the past year, many advisors rely solely upon a simple password as the primary access control to preventing the theft of Protected Data stored in a cloud application. Simultaneously, those passwords are often re-used across the internet from one application to the next. Often, the username is something as simple as the advisor's e-mail address.

Vendor Breaches Can Prove Costly for Financial Institutions

According to a study commissioned by eSentire in 2019, nearly half of firms suffer data breaches at hands of vendors.[4] Even though the majority of respondents felt confident in the vendor to keep their data safe, nearly half (44 percent) of firms had experienced a significant, business altering data breach caused by a vendor. Human error and stolen passwords accounted for 26 percent of the breaches, while malware played a key role in half of the attacks. Of the nearly 250 companies that experienced a breach, 32 percent affected personal identifiable data, 29 percent included payment information, and 24 percent exposed proprietary business data. According to the study, only 15 percent of firms reported that their vendor notified them when a breach occurred.

As highlighted in the next section, regulators have placed significant emphasis on the importance third-party risk management plays in an effective cybersecurity program. In November of 2016, FINRA fined Lincoln Financial Securities Corporation ("LFS") $650,000 for its failure to adequately supervise FinTech Vendors tasked with electronic storage of customer records and electronic preservation and retention of customer consolidated reports.[5] The penalty came on the heels of FINRA previously fining Lincoln $600,000 for other information security deficiencies in 2012.

Creating a Culture of Cybersecurity to Assist in Mitigating Human / Manual Error

Human error and cybersecurity attacks are very much linked. According to the 2022 Verizon Data Breach Investigations Report (DBIR)[6], 82% of data breaches involved a human element. The study reported, "Human error continues to play a large part in data breaches. 13% of breaches involved misconfigurations, mostly of cloud storage facilities, and 82% of all data breaches analyzed in the past 12 months involved a human element. Phishing is a popular social engineering method, during which cybercriminals send email scams to trick victims into providing credentials and sensitive business information. Phishing training and simultaneously delivering context-based education to employees / advisors has proved useful in combating phishing attempts.

Cybercriminals prey upon human error, IT security complacency, and technical deficiencies present in computer networks all over the world. Once they are inside a network their process is almost always the same: establish continued access, escalate or obtain administrator privileges, move slowly and quietly to map the entire network, look for open vulnerabilities, locate critical assets, and exfiltrate the data undetected for as long as possible.

To err is human. Set your staff up for success. Perform routine training to engage employees to look for and communicate potential incidents. Monitor what processes access personal data and add in redundant controls so that a single mistake doesn't result in a breach or data leak. Implement a routine checklist for general security hygiene and

[4] eSentire, "Nearly half of firms suffer data breaches at hands of vendors"; April 2019
[5] Databreaches.net, "FINRA Fines Lincoln Financial Subsidiary $650,000 For Cybersecurity Shortcomings"; November 2016
[6] Verizon, "2022 Verizon Data Breach Investigations Report (DBIR)", April 2022

have sys admins make sure that the systems you build deploy patches and updates in a timely fashion. Automate anything you can as this reduces the human error associated with many breaches we see. Conduct routine scans to discover misconfigurations before a threat actor does.

Solutions Exist

Most independent broker dealers, investment advisors, and their affiliated financial advisors use a diversity of third-party vendors in order to run their businesses. Security Basecamp performs third-party cybersecurity due diligence on behalf of such organizations, and it is commonplace for the typical independent broker dealer to have over 200 vendors upon which to conduct on-going vendor risk management. This is a daunting task for the typical firm. Knowing how and when a vendor may be breached is exceptionally complicated. It is hard enough to mitigate breaches in our own organizations let alone third parties which by their very nature we don't directly manage.

Most firms do not have the resources required to execute a Third-Party Risk Management (TPRM) program nor the knowledge of how to build such a program. This report outlines best practice recommendations for building such a program. When constructing a TPRM program, it is essential to start with a list of standards to which vendors being assessed will be held. The financial services industry is heavily regulated and as such, it is paramount to begin with a strong understanding of the regulatory standards to which vendors should be held. As such, the next section of this report provides high-level notable regulatory guidance regarding vendor risk management in our industry.

Many firms choose to outsource the function of vendor cybersecurity due diligence to knowledgeable experts that have a defined approach and sets of tools for performing the work. Consulting firms such as Security Basecamp and others have built vendor cybersecurity due diligence methodologies that are executed on behalf of our clients.

Simultaneously, cleverDome is highlighted as a case study throughout this report. cleverDome has created a community-built solution for the wealth management industry. cleverDome's secures Protected Data by taking it off the open Internet and "under the Dome." TM The Dome is a multi-faceted cybersecurity risk management platform. A key component of the Dome is vendor risk management. cleverDome maintains a customized questionnaire based on the cleverDome Minimum Cybersecurity Standards which are based on industry standards (i.e. FINRA, SEC), applicable regulation (i.e. NY-DFS, NAIC Model Law, California Consumer Protection), and were created by the collaborative work of cleverDome Members and other wealth management industry constituents. cleverDome has partnered with Security Basecamp to facilitate the vendor risk management process for cleverDome Members. In addition to applicable regulatory guidance and laws, applicable cybersecurity standards have been incorporated including explicitly the ISO/IEC 27000 and NIST standards. All vendors are inventoried and important details about each vendor is stored in a centralized system. cleverDome has customized a questionnaire to incorporate the cleverDome Minimum Cybersecurity Standards and to facilitate vendor attestations to regulatory requirements and security best practices specific to the regulated wealth management industry.

cleverDome acts as a trust broker by provisioning cleverDome Members to exchange Protected Data under the Dome. Each cleverDome Member is required to meet the cleverDome Minimum Cybersecurity Standards and complete the due diligence process to enter the Dome.[7] Notable regulatory guidance upon which cleverDome has based its standards is highlighted in the Appendix of this report.

[7] cleverDome, https://www.cleverdome.com/ (web); April 2022.

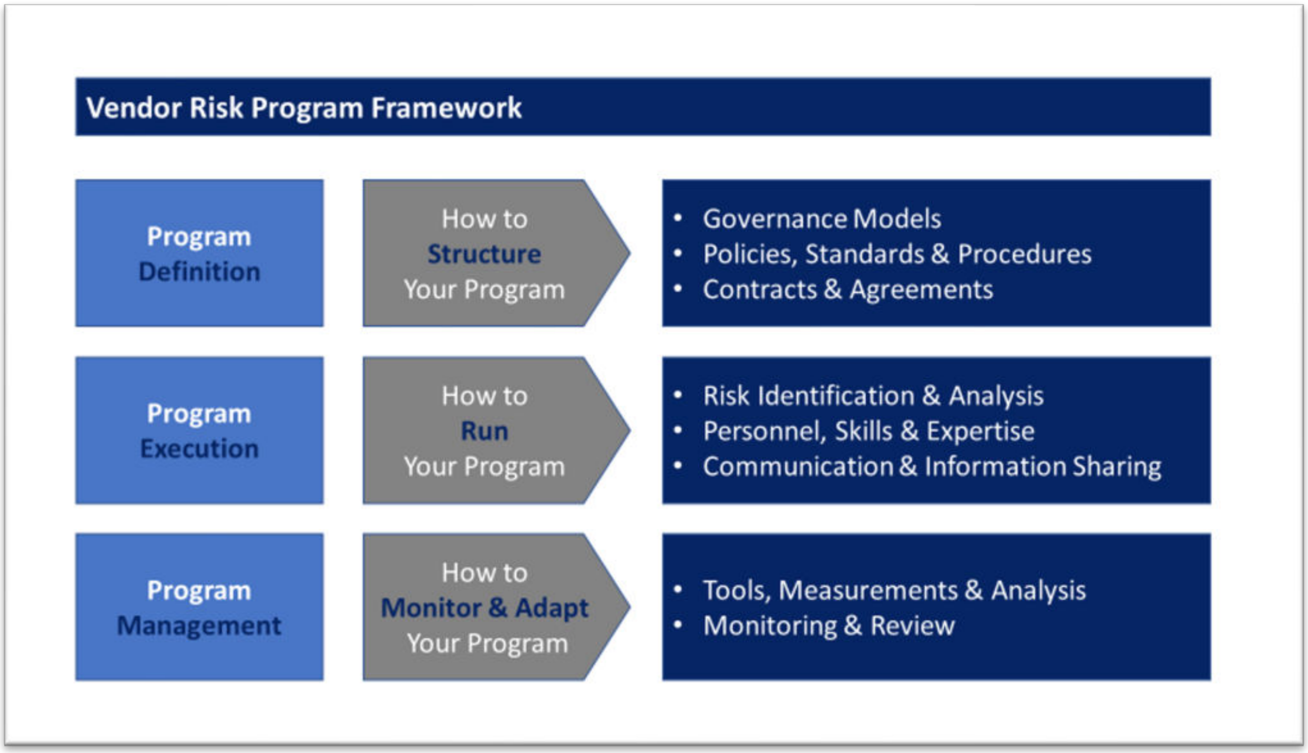
BEST PRACTICE CONSIDERATIONS FOR PERFORMING VENDOR CYBERSECURITY DUE DILIGENCE

Performing effective vendor risk management can vary from one organization to the next. To some extent, this is acceptable. The professions of engineering, medicine, accounting, and many others are not necessarily applied (i.e. performed) identically, yet predictably yield intended outcomes. That said, any professional process should contain some essential foundational elements.

Essential Third-Party Risk Management Program Building Blocks

The Vendor Risk Management Framework shown below, taken from the Shared Assessments CTPRP Workshop, is illustrative and useful in introducing the basic building blocks required for effective vendor cybersecurity due diligence.

Figure 2: Defining Your Program Foundation[8]



Vendor Risk Program Framework

Program Definition — How to Structure Your Program
- Governance Models
- Policies, Standards & Procedures
- Contracts & Agreements

Program Execution — How to Run Your Program
- Risk Identification & Analysis
- Personnel, Skills & Expertise
- Communication & Information Sharing

Program Management — How to Monitor & Adapt Your Program
- Tools, Measurements & Analysis
- Monitoring & Review

Third-Party Risk Management Program Governance

Governance is where it all starts. It is important to write out the “objectives of your program” and to state “who is responsible for what?”. Most anything that involves a team working together to accomplish something requires us to simply answer the questions “why are we doing this?”, “what are our goals?”, “how will we achieve them?”, and “who is responsible for doing what and when?”. Define clear roles and responsibilities for the third-party risk management program. Create a risk management framework to focus your approach. “Right-size” your structure based on a risk assessment. At a minimum, your Third-Party Vendor Management Program should cover items such as:

- Maintaining an active list of vendors and their related cybersecurity risk (e.g. vendors accessing / storing Protected Data may be judged more of a risk than those vendors that don’t),
- Establishing a process for onboarding new vendors that includes a focus on contract provisions, technical controls, periodic risk assessments, vendor training and termination provisions.

[8] Shared Assessments, Vendor Risk Program Framework, Certified Third-party Risk Professional (CTPRP) Workshop; January 2019

- Evaluating the adequacy of vendor cybersecurity practices (and in a commercially reasonably way that most efficiently leverages both the time and resources of firm resources and those of its vendor partners; many firms choose to outsource this function,
- Providing relevant guidelines for due diligence (e.g. vendors understand to what “minimum cybersecurity standards” they are being held and then a commercially reasonable approach for performing / evidencing cybersecurity due diligence, etc.);
- Prescribing essential technical protections for both a variety of security concentration areas including access controls (e.g. multi-factor authentication “MFA”) and data loss prevention (e.g. Full Disk Encryption “FDE” of devices storing Protected Data),
- Requiring notification to your firm in the event of a cybersecurity event,
- Requiring representations and warranties addressing a third-party’s cybersecurity policies and procedures,
- Setting contractual standards to govern vendor relationships; make sure to include “Right to Audit” clauses in all agreements,
- Defining a vendor termination processes to ensure access is managed in accordance with vendor contract status.

Contracts & Agreements: Useful Terms

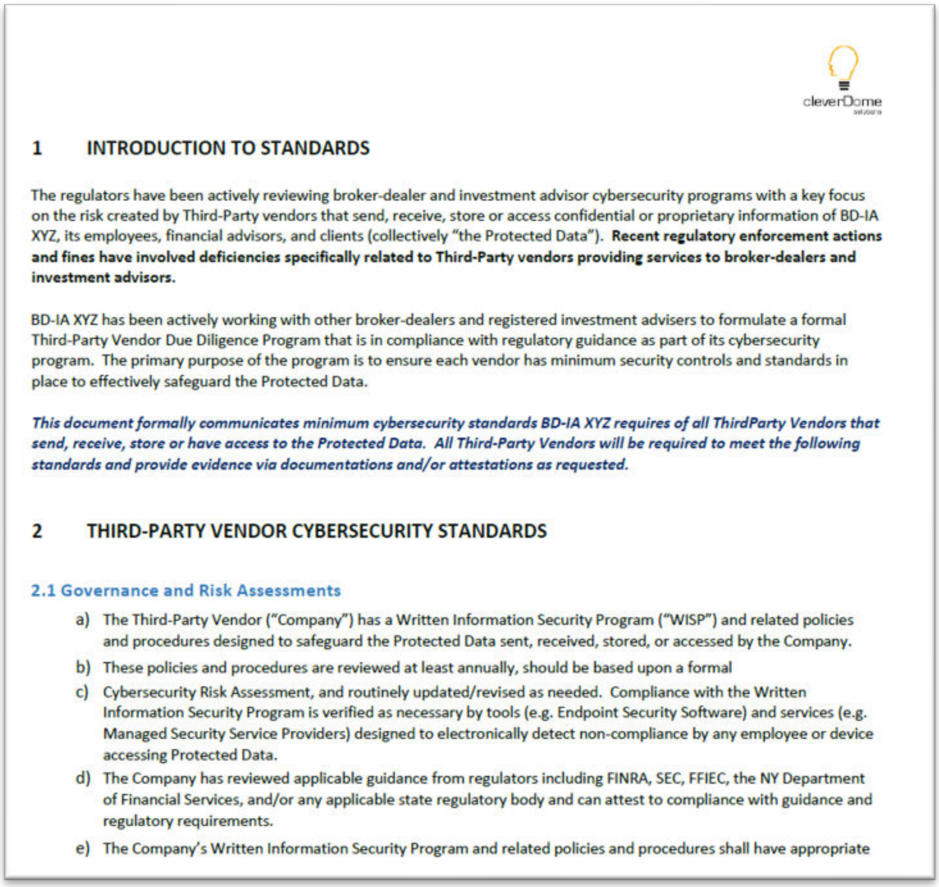
In establishing and reviewing contracts, the following guidance on cybersecurity provisions should at a minimum be considered:

- Non-disclosure agreements/confidentiality agreements: This language outlines confidential material, knowledge or information that the parties exchange, such as customer Personally Identifiable Information (“PII”) or company trade secrets. The parties agree not to share further or disclose information obtained under the contract.
- Data storage, retention and delivery: This language describes how firm data should be stored and transmitted while on a vendor’s system. This may include encryption requirements, requirements as to the type and location of servers used, and business recovery practices.
- Breach notification responsibilities: This language addresses the manner and timing of the vendor’s notification to the data owner of a security breach and the requirements as to who is responsible for notifying customers along with any related costs. Contract language also would include the definition of a breach as it relates to the data or systems involved.
- Right-to-audit clauses: This language gives the data owner the ability to perform physical audits of the vendor’s facilities and related controls. These clauses also might outline the vendor’s responsibility for having a third-party test of the vendor’s controls.
- Vendor employee access limitations: This language defines which vendor employees have access to firm data. Typically, this language also documents the approval process for granting this access, *e.g.*, who at the firm would approve employee access to restricted data.
- Use of subcontractors: This language outlines any subcontractors that the vendor will use and that would have access to firm data. It also addresses the controls that the vendor would require at any subcontractor, for instance regarding employee data access or data encryption. Typically, controls expected to be present at the vendor would also be required at the subcontractor.
- Vendor obligations upon contract termination: This language addresses requirements regarding the destruction or return of any data stored at the vendor’s physical locations, including how quickly any data would be disposed of. It also includes language related to removing employee access to the data.

Standards: The Foundational Element Required

Standards are the most foundational element of an effective third-party risk management program. They literally drive “everything”. Standards are “what you execute, upon which you take action, upon which you measure adherence” and in order to perform due diligence they must be well constructed. Standards, like the attestation questionnaires used as the initial basis for determining their being met or not, are organized into a series of “control areas” (e.g. Governance and Risk Assessments, Asset Management, Access Control, Network Security, etc.). An excerpt from the cleverDome standards is included below for illustrative purposes.

Figure 3: Excerpt from cleverDome Third-Party Vendor Cybersecurity Standards[9]



cleverDome

1 INTRODUCTION TO STANDARDS

The regulators have been actively reviewing broker-dealer and investment advisor cybersecurity programs with a key focus on the risk created by Third-Party vendors that send, receive, store or access confidential or proprietary information of BD-IA XYZ, its employees, financial advisors, and clients (collectively “the Protected Data”). **Recent regulatory enforcement actions and fines have involved deficiencies specifically related to Third-Party vendors providing services to broker-dealers and investment advisors.**

BD-IA XYZ has been actively working with other broker-dealers and registered investment advisers to formulate a formal Third-Party Vendor Due Diligence Program that is in compliance with regulatory guidance as part of its cybersecurity program. The primary purpose of the program is to ensure each vendor has minimum security controls and standards in place to effectively safeguard the Protected Data.

This document formally communicates minimum cybersecurity standards BD-IA XYZ requires of all ThirdParty Vendors that send, receive, store or have access to the Protected Data. All Third-Party Vendors will be required to meet the following standards and provide evidence via documentations and/or attestations as requested.

2 THIRD-PARTY VENDOR CYBERSECURITY STANDARDS

2.1 Governance and Risk Assessments

a) The Third-Party Vendor (“Company”) has a Written Information Security Program (“WISP”) and related policies and procedures designed to safeguard the Protected Data sent, received, stored, or accessed by the Company.

b) These policies and procedures are reviewed at least annually, should be based upon a formal

c) Cybersecurity Risk Assessment, and routinely updated/revised as needed. Compliance with the Written Information Security Program is verified as necessary by tools (e.g. Endpoint Security Software) and services (e.g. Managed Security Service Providers) designed to electronically detect non-compliance by any employee or device accessing Protected Data.

d) The Company has reviewed applicable guidance from regulators including FINRA, SEC, FFIEC, the NY Department of Financial Services, and/or any applicable state regulatory body and can attest to compliance with guidance and regulatory requirements.

e) The Company’s Written Information Security Program and related policies and procedures shall have appropriate

Standards exist so that a risk assessor knows what to inspect and verify. Simultaneously, without standards, the vendors being inspected and verified have no idea to what they are being held accountable. The financial services industry is heavily regulated. The basis of appropriate standards needs to include regulatory insight. See Legal & Regulatory Resources in the appendices of this document for a synopsis of essential regulations of which we should minimally be cognizant. Additionally, certain best practices have evolved, and continue to evolve, as it relates to the execution of a sound cybersecurity program. See Cybersecurity Standards & Frameworks in the appendices of this document. Numerous standards have evolved both broadly within our economy (e.g. the NIST Cybersecurity Framework) or more specifically to an industry’s requirements (e.g. the cleverDome standards).

[9] cleverDome BD/IA Cyber Consortium: Minimum Cybersecurity Standards for Third-Party Vendors. Note: cleverDome maintains these standards and works with industry constituents to evolve and adapt them as required. For example, should standards change measurably due to new regulation or security control best practice updates, then vendors upon which due diligence is performed on behalf of cleverDome members receive updated questionnaires to reflect changes in the cleverDome standards.

Control Areas (i.e. Security Concentrations Areas) for Analysis

Standards should be assessed comprehensively and logically. Security concentration areas group controls expected to be in place at a vendor in order to assess their relative adherence to the standards. The specific categories and grouping vary by the Cybersecurity Standards & Frameworks highlighted in this report's appendices (and thus also the questionnaires similarly referenced).

Below is a summarization of control areas for illustrative purposes. Control Areas are presented for both the cleverDome Standards and the Shared Assessments SIG Questionnaire. It is our experience that in the "hands of an experienced" assessor, both approaches can work. That said, in reviewing the list it should be apparent that the cleverDome standards and questionnaires have been constructed and tailored to meet the specific needs of the regulated financial services industry. Standards, and applicable questionnaire-driven attestations, gather evidence of a vendor's compliance with specific elements common to what our regulators would expect. Security Basecamp has a mapping for control areas across the various Cybersecurity Standards and Frameworks including those listed in this report's appendices and more.

Figure 4: Security Concentration Control Areas for Analysis

cleverDome Control Areas	Shared Assessments SIG Control Areas
• Governance and Risk Assessment • Device Management • Access Rights and Controls • Encryption and Data Loss Prevention • Data Privacy and Integrity • Vulnerability Assessments / Scans and Penetration Tests • Compliance • Audit Trail /Logging • Information Systems / Application Acquisition, Development and Related Security • Communications and Operations Management • Cybersecurity Insurance • Vendor Management • Human Resources / Training and Monitoring • Money Movement Controls • Business Resiliency, Continuity and Disaster Recovery • Physical Environment • Cloud Management and Security • Security Incident Detection, Monitoring and Incident Response • Supporting Communications with Regulatory Organizations	• Governance and Risk Assessment • Information Security Policy • Organizational Security • Asset Management • Human Resources Security • Physical and Environmental Security • Operations Management • Access Control • Application Security • Incident Event and Communications • Business Resiliency • Compliance • End User Device Security • Network Security • Privacy • Threat Management • Server Security • Cloud Security

Vendor Inventories & Risk Classifications: Focusing Your Effort

The Inventory Maintenance process involves developing a complete list of all vendors and ideally essential details about them (e.g. primary contacts, contract dates, terms and conditions, etc.). Simultaneously, vendors should be categorized as to the risk they present to your organization. What is the nature of the services provided? Is Protected Data stored or accessed or transmitted? Does the vendor facilitate the potential movement of money from or between accounts? Although this process of inventorying all vendors and assessing their relative risk seems basic in nature, it is our experience that most organizations in our industry are at least somewhat challenged to produce an accurate list of all vendors along with the contracts outlining the terms and conditions of their relationship.

Attestations (i.e. Third-Party Risk Management Questionnaires)

Setting effective standards is a daunting task. Yet, they are required in order to ensure compliance with applicable regulatory requirements and in order to ensure the protection of confidential information. Once standards are set, questionnaires should be constructed that require vendors to attest to whether they meet specific standards or not. Ideally, risk assessors will qualify vendors prior to asking each to answer a comprehensive set of attestations. Not every vendor provides access to, stores, nor transmits Protected Data and/or offers the ability to perform a financial transaction. Vendors, or all organization alike, can expect to attest to hundreds and hundreds of specific items that set the basis for compliance with the standards required for 1) regulatory requirements and 2) sound information security practices. Make sure to minimize busy-work on behalf of your vendors and to spend the most time analyzing those vendors which truly represent risk to your organization. As standards are adapted to reflect evolving requirements, questionnaires should be expected to evolve as well. A process (and toolset) should be created to capture attestations across your vendor population and record changes in those attestations over time.

Questionnaires received by vendors today across the industry vary immensely. Popular FinTech software companies have literally had to hire teams of people to simply respond to questionnaires of varying usefulness. It is our experience that the most commonly used questionnaire today is the Shared Assessments SIG. It is a complex questionnaire (a Full and Lite version exists) requiring professional expertise in its use and application. The Shared Assessments organization has created a Certification Program that professionals can complete resulting in the CTPRP (Certified Third-Party Risk Professional) designation. That said, the Shared Assessment SIG is used across industries and without thoughtful application may or may not result in an assessor determining whether a vendor is compliant with applicable financial service industry regulatory guidance. Additionally, it is our experience that many that complete the Shared Assessment SIG are not necessarily equipped to meaningfully complete it given its relatively complex nature.

Via the cleverDome process, vendors answer an initial questionnaire (Part A) that qualifies the vendor and is used to substantiate whether the vendor needs to complete a more exhaustive questionnaire (Part B). Part A takes the typical vendor 3-5 minutes to complete. Part B, 60-90 minutes to complete depending upon the vendor and the attestor's (i.e. vendor staff completing the questionnaire) knowledge of the vendor's cybersecurity program. This simple process of qualification assists in minimizing effort to providing the "least" amount of information necessary. In contrast, it is our experiences that completing the Shared Assessment SIG can take significantly more time (e.g. 1-2 weeks for a thoughtfully completed SIG-Full).

Evidencing Attestations Through Analysis of Supporting Documentation

Once the vendor has made attestations to represent performance (or non-performance) of each of the specific standards, the risk assessor should analyze supporting documentation to verify the attestations made. As Ronald Reagan popularly noted, we "trust, but verify". Requests for supporting documentation should be made at the same time the questionnaire is provided to the vendor. Supporting documentation helpful to gather may include:

a. Cybersecurity Program Documentation: Collect Written Cybersecurity Policies and Procedures for protecting information and preventing fraud. Ideally, the vendor will have what we call a "distributable version" of their written program (versus providing full versions for inspection which would in essence is akin to providing "the keys to the kingdom".

b. Other Questionnaires. It can be useful to receive previously completed questionnaires should they exist (for example, Shared Assessment SIG - preferably the full version vs. the lite version. Comparing answers from one questionnaire to the next can illustrate areas for deeper inspection. That said, as stated in the previous section, be cognizant of related comments previously made.
c. Electronic Scans / Testing / Results: Penetration Tests and/or Vulnerability Scans should have been previously completed and distributable summaries should be analyzed. If they have not been performed, that will be illustrative in and of itself and the assessor should make plans to have vulnerability scans completed and penetration tests executed if applicable. Additionally, some services are evolving that provide routinely available scans of public facing threats or vulnerabilities scans for a vendor's domain. Electronic scanning is an evolving area that will likely prove revolutionary in the future. For example, solutions such as BitSight Security Ratings allow organizations to continuously monitor the security performance of all its third-parties, vendors, and suppliers. Hackers use automated bots to scan the public internet to find "low hanging fruit" or perform dark web scans to purchase stolen credentials, so it should be assumed that third-party risk assessors can benefit from similar techniques. Organizations such as cleverDome aim to remove "public exposures" facing organizations by taking devices and data "off the open internet" and this is also an essential element for further securing our industry and its constituents.

As the assessor reviews supporting documentation and the results of vendor attestations via the questionnaires, requests should be made for relevant evidence to support attestations made or items of incongruency. This is particularly important when analysis performed by an experienced assessor would cause concern when an answer doesn't seem to make sense (e.g. the vendor states they have a cybersecurity program, but can't provide a written summary or the vendor states they have a comprehensive cybersecurity program, but there is not a CISO or information security function within the organization.).

Evidencing Attestations Through Analysis of Third-Party Audit Reports or Security Certifications

Notable Cybersecurity Standards and Frameworks are highlighted in the appendices of this document. Professionally leveraging the results of these standards and frameworks is an essential element of the risk assessor's work. Notable reports and certifications include those listed below. Others exist (e.g. HIPPA) and an experienced professional should use judgement as to which would be most applicable or helpful in effectively performing due diligence on a particular vendor.

ISO 27001 Certifications

ISO/IEC 27001 specifies a management system that is intended to bring information security under management control and gives specific requirements. Organizations that meet the requirements may be certified by an accredited certification body following successful completion of an audit. The work typically required to achieve this certification can take many years to institute and then thoroughly audit. ISO/IEC 27001 requires that management:

- Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;
- Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and
- Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

System and Organizational Controls (SOC Reports for Service Organizations and/or Cybersecurity).

Developed by the American Institute of CPAs (AICPA), SOC defines criteria for managing customer data based on five "trust service principles"—security, availability, processing integrity, confidentiality and privacy. The American Institute of Certified Public Accountants (AICPA) launched the SOC assessment report framework in 2011, and with that came three (3) new reporting options: SOC 1, SOC 2, and SOC 3. Together, these three (3) reporting options replaced the one-size-fits-all SAS 70 auditing standard that had been in use since 1992. The SOC 2 standard is now arguably the most widely recognized report type used because more and more technology-oriented businesses are undergoing the annual SOC 2 compliance (e.g. data centers, Software as a Service (SaaS), managed security service providers, etc.) audit process.

It is important to realize that SOC Reports are unique to each organization (i.e. there is a range of scope / utility related to SOC Reports and the quality is somewhat dependent upon which organization performs the audits). Additionally, going through the SOC process can be arduous for many "startups" software firms and to require it as a universal standard could potentially stifle innovation. Similar to ISO 27001 Certifications, achieving a clean audit as represented by a SOC Report that is broadly scoped to include all applicable controls can take multiple years to achieve.

Again, experienced and trained professionals with an acumen for detailed analysis combined with judgement should be involved in performing third-party risk assessments. The most common report we request and use when performing our analysis is a SOC 2 Type II as it reports on the operational effectiveness of the vendors information security program and related controls. The vendor is either given a Qualified or Unqualified Opinion by an accredited auditor and numerous controls are assessed as to being effectively performed or not over a period typically at least 6 months in duration.

Interactions with the Vendor (e.g. Remote Verification)

During the "trust, but verify" stage of a vendor's review, conversations should be held with vendors to answer questions that can't be readily addressed via the review of written supporting documentation or third-party audit reports. A trained professional can readily ascertain "the truth" in conversations with vendors. By this point in a vendor's review, hundreds of questions will have been answered by the vendor that can either be corroborated or determined to be false. Security Basecamp utilizes a process whereby attestations are either "cleared" one by one or left open as a question to be answered via evidencing or conversations with the vendor. If an attestation cannot be "cleared", it results in a risk to be either classified as either Moderate or High. High Risk items result in a vendor failing the Risk Assessment process (i.e. Not approved for use). Moderate Risk items require the vendor to commit to resolving the item in the near-term.

Performing On-Site Inspections

Sometimes it may be necessary to go on site to complete due diligence on a vendor. Attestations may be difficult to verify due to the length of time a vendor has been in operation or the vendor may be unable or unwilling to provide the information required to verify attestations. On-site inspections can be performed by third-party assessors and planning should be completed to ensure time is well spent.

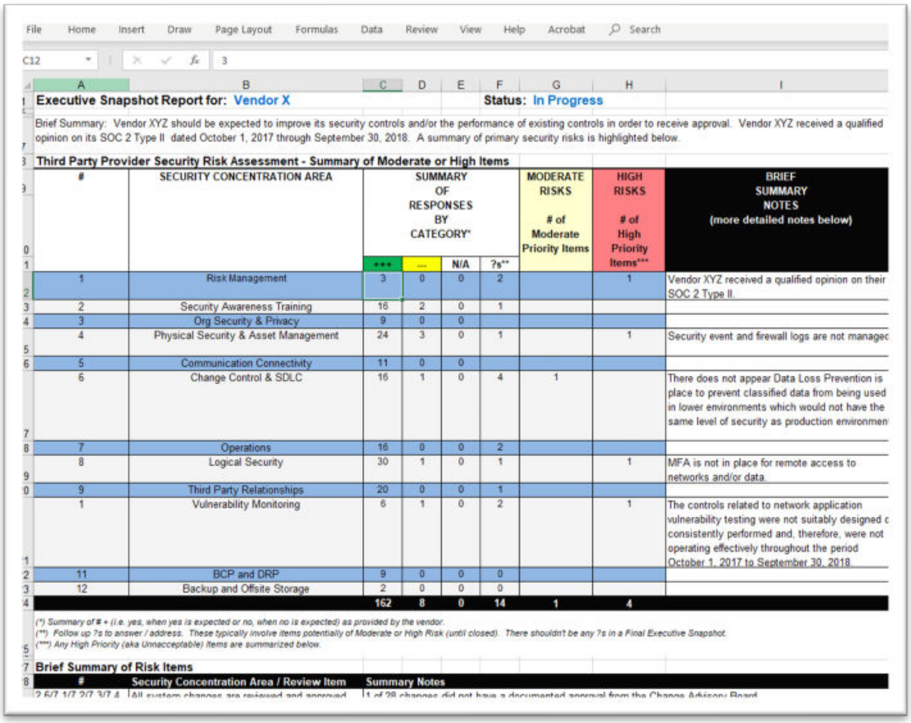
Write Vendor Risk Assessment Summary Reports

cleverDome creates risk reports for vendors that complete the attestations. As described in this report (illustratively shown below), the on-line repository of attestation reports across the vendor population serves as the basis for completing the rest of the cybersecurity due diligence steps.

Supporting documentation and other evidentiary information can be uploaded into the on-line repository. The Scored Risk Reports received across a population of hundreds of vendors can serve to compare an organization's vendor population relative risk ratings and to focus action on those vendors needing most attention.

As vendor attestations are reviewed in detail, evidenced, and essential risks identified, a process should be followed to summarize the results of the vendor review. This process should facilitate clear communication with both firm management and the vendor; most importantly, remediation steps required to address risks identified. Security Basecamp follows a process of "clearing all attestations" that results in a summary of risk items. Moderate Risk items are those that result in the "conditional approval" of a vendor assuming they commit to remediating those risks in a given period. Think of "Moderate Risk" items in a similar fashion to "heightened supervision" in broker dealer nomenclature. High Risk items are those that result in risks that the assessor deems as unacceptable. Unless High Risk items are remediated, the assessor recommends termination of the vendor relationship. Some firms may choose to override the assessor and "accept" risks identified. This should be done in careful consultation with industry experts.

Figure 6: Security Basecamp Approach to Summarizing (& Tracking Vendor Remediations of Risk Items)



Executive Snapshot Report for: Vendor X **Status:** In Progress

Brief Summary: Vendor XYZ should be expected to improve its security controls and/or the performance of existing controls in order to receive approval. Vendor XYZ received a qualified opinion on its SOC 2 Type II dated October 1, 2017 through September 30, 2018. A summary of primary security risks is highlighted below.

Third Party Provider Security Risk Assessment - Summary of Moderate or High Items

#	SECURITY CONCENTRATION AREA	SUMMARY OF RESPONSES BY CATEGORY*				MODERATE RISKS # of Moderate Priority Items	HIGH RISKS # of High Priority Items***	BRIEF SUMMARY NOTES (more detailed notes below)
		+++	---	N/A	?s**			
1	Risk Management	3	0	0	2		1	Vendor XYZ received a qualified opinion on their SOC 2 Type II.
2	Security Awareness Training	16	2	0	1			
3	Org Security & Privacy	9	0	0				
4	Physical Security & Asset Management	24	3	0	1		1	Security event and firewall logs are not managec
5	Communication Connectivity	11	0	0				
6	Change Control & SDLC	16	1	0	4	1		There does not appear Data Loss Prevention is place to prevent classified data from being used in lower environments which would not have the same level of security as production environmen
7	Operations	16	0	0	2			
8	Logical Security	30	1	0	1		1	MFA is not in place for remote access to networks and/or data.
9	Third Party Relationships	20	0	0	1			
1	Vulnerability Monitoring	6	1	0	2		1	The controls related to network application vulnerability testing were not suitably designed c consistently performed and, therefore, were not operating effectively throughout the period October 1, 2017 to September 30, 2018.
11	BCP and DRP	9	0	0	0			
12	Backup and Offsite Storage	2	0	0	0			
		162	8	0	14	1	4	

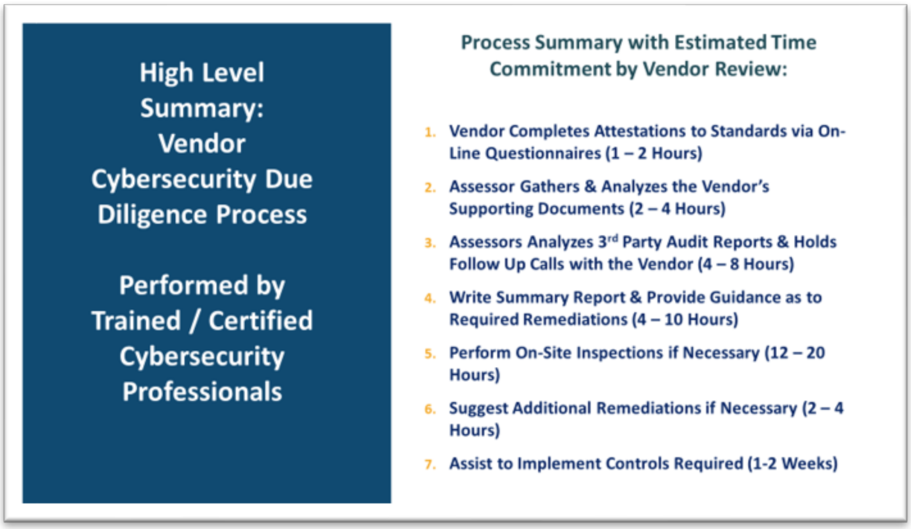
(*) Summary of # + (i.e. yes, when yes is expected or no, when no is expected) as provided by the vendor.
(**) Follow up ?s to answer / address. These typically involve items potentially of Moderate or High Risk (until closed). There shouldn't be any ?s in a Final Executive Snapshot.
(***) Any High Priority (aka Unnacceptable) Items are summarized below.

Brief Summary of Risk Items

#	Security Concentration Area / Review Item	Summary Notes
2.6/7 1/7 2/7 3/7 4	All system changes are reviewed and approved	1 of 28 changes did not have a documented approval from the Change Advisory Board

A summary overview of the process followed in performing our vendor cybersecurity due diligence process is shown below. The specific amount of time allocated to consultative vendor due diligence review varies depending upon the risk categorization of the vendor and the relative cybersecurity program maturity of a given vendor.

Figure 7: High-Level Summary of the Vendor Cybersecurity Due Diligence Process



High Level Summary: Vendor Cybersecurity Due Diligence Process

Performed by Trained / Certified Cybersecurity Professionals

Process Summary with Estimated Time Commitment by Vendor Review:

1. Vendor Completes Attestations to Standards via On-Line Questionnaires (1 – 2 Hours)
2. Assessor Gathers & Analyzes the Vendor's Supporting Documents (2 – 4 Hours)
3. Assessors Analyzes 3rd Party Audit Reports & Holds Follow Up Calls with the Vendor (4 – 8 Hours)
4. Write Summary Report & Provide Guidance as to Required Remediations (4 – 10 Hours)
5. Perform On-Site Inspections if Necessary (12 – 20 Hours)
6. Suggest Additional Remediations if Necessary (2 – 4 Hours)
7. Assist to Implement Controls Required (1-2 Weeks)

Ultimately, the goal of the process is to identify threats and vulnerabilities needing to be addressed, a resolution to those items not meeting applicable standards, and simultaneously a more compliant / secure third-party vendor relationship.

The balance of this report includes links to Additional Resources utilized in writing this report.

ABOUT SECURITY BASECAMP

Security Basecamp is a consulting firm focused exclusively in the financial services industry. We partner with executives and managers to facilitate effective business planning and help you competitively leverage technology for profitable growth. Our mission is to help financial services firms solve their most challenging strategic business issues through critical thinking, rigorous project management, and/or the savvy use of practical technologies.

Collectively, our consultants have managed more than 100 strategy, operations, technology, compliance, and business development projects over the past 25 years. We bring a business-oriented approach to completing cybersecurity projects and the technical acumen to work effectively with your internal IT staff. We help you manage the cybersecurity analysis, action planning, and execution that your busy management team doesn't have the time or resources to lead. We offer three primary cybersecurity services: 1) Risk Assessments, 2) a vCISO Service, and 3) Vendor Cybersecurity Due Diligence. To learn more, visit our website www.securitybasecamp.com or call (949) 330-0899.

ABOUT CLEVERDOME

cleverDome. ™ is an Arizona Benefit Corporation (B Corporation) that operates as a Co-Op. Members include managed security service providers, software service vendors, custodians, broker dealers, registered investment advisers, financial advisors and ultimately their investor clients.

As a B Corporation, its mission is to protect confidential consumer information through safe, reliable and fast Internet connections. cleverDome CEO and co-founder Aaron Spradlin and Chief Risk Officer and co-founder Bridget Gaughan established cleverDome as a B corporation to create a solid and permanent commitment to delivering a community-based solution to protect confidential client information. cleverDome provides a fundamental model for the future of secure trust networks: the unification of end-point protection with a secure communication layer under a common due diligence standard. This revolutionary model is built on a community-driven platform in collaboration with financial services industry thought-leaders. The Dome is powered by NetFoundry™, a Tata Communications business incubated in Tata Communications' “Shape the Future” program. To learn more, visit www.cleverDome.com or call (480) 566-8565.

AUTHOR INFORMATION

Paul Osterberg
Managing Director, Security Basecamp
(949) 330-0899
posterberg@securitybasecamp.com

APPENDIX

Notable Regulatory Guidance

NASD (n/k/a FINRA) Rules of Fair Practice have always required confidential treatment of customer information. Regulation S-P[10] further strengthened this requirement. Brokers, dealers, investment companies, and investment advisers registered with the SEC are required to:

1. Adopt reasonably designed written policies and procedures addressing administrative, technical and physical safeguards for the protection of customer information and records; and
2. Protect against any anticipated threats or hazards to the security or integrity of customer records and information, and against unauthorized access to or use of customer records or information.

Business practices have evolved significantly since the time that FINRA and the SEC originally issued guidance regarding the protection of customer information. Each, as summarized below, have issued detailed cybersecurity reports to regulated institutions that provide guidance regarding vendor management. States, most notably New York (effective now) and California (to be effective in early 2020), have enacted legislation and those of the New York Department of Financial Services (NY-DFS) are highlighted below.

FINRA

FINRA published a Report on Cybersecurity Practices[11] in the broker dealer industry to highlight effective practices that firms should consider to strengthen their cybersecurity programs. FINRA stated that the report “does not create any new legal requirements or change any existing regulatory obligations. Our expectation is that firms will use the report to assess and strengthen their cybersecurity practices.”

The report has a section dedicated to Vendor Management. FINRA stated, “Broker dealers typically use vendors for services that provide the vendor with access to sensitive firm or client information or access to firm systems. Firms should manage cybersecurity risk exposures that arise from these relationships by exercising strong due diligence across the lifecycle of their vendor relationships.”[12] Key points of the section on Vendor Management include the following.

- Firms should manage cybersecurity risk that can arise across the lifecycle of vendor relationships using a risk-based approach to vendor management. Effective practices to manage vendor risk include:
  - performing pre-contract due diligence on prospective service providers. This due diligence provides a basis for the firm to evaluate whether the prospective vendor’s cybersecurity measures meet the firm’s cybersecurity standards;
  - establishing contractual terms appropriate to the sensitivity of information and systems to which the vendor may have access, and which govern both the ongoing relationship with the vendor and the vendor’s obligations after the relationship ends;
  - performing ongoing due diligence on existing vendors;
  - including vendor relationships and outsourced systems as part of the firm’s ongoing risk assessment process;
  - establishing and implementing procedures to terminate vendor access to firm systems immediately upon contract termination; and
  - establishing, maintaining and monitoring vendor entitlements to align with firm risk appetite and information security standards.

[10] Morrison & Foerster LLP, Broker Dealer Cybersecurity: Protect Yourself or Pay the Price, January 10, 2014: Regulation S-P became effective in November 2000, and compliance with the rules and regulations has been mandatory since July 1, 2001.

[11] FINRA, *Report on Cybersecurity Practices* (February 3, 2015).

[12] Ibid, page 2.

- Analyzing FINRA’s requirements makes it essential that vendor risk management be an on-going activity and that it involves the application of cybersecurity standards. Key problems facing our industry include the reality that first, most firms (in particular, small financial advisory firms), do not have the resources required to effectively perform cybersecurity due diligence of their vendors and second, often do not know the standards that should be applied.
- Firms across many industry sectors rely on third-party vendors for a range of services. As recent incidents have shown, these same vendors can also be a significant source of cybersecurity risk. These risks can arise in different ways, for example, if a vendor or one of its employees misuses firm data or systems, if the vendor itself is subject to a cyberattack that compromises vendor systems or firm data, or if an attack on a vendor becomes a vector for an attack on a firm’s systems. Firms need an effective vendor management program in place to help guard against these risks.[13]
- The Notice to Members footnoted in this statement relates to “outsourcing” and in summary, broker dealers or regulated entities FINRA wished to “remind members that, in general, any parties conducting activities or functions that require registration under NASD rules will be considered associated persons of the member, absent the service provider separately being registered as a broker dealer and such arrangements being contemplated by NASD rules (such as in the case of clearing arrangements)” and that “in addition, outsourcing an activity or function to a third-party does not relieve members of their ultimate responsibility for compliance with all applicable federal securities laws and regulations and NASD and MSRB rules regarding the outsourced activity or function.” In other words, it is the regulated institution that is being held accountable (not necessarily the third-party to which an important business function is being outsourced).

Office of Compliance Inspections and Examinations (OCIE) of the U.S. Securities and Exchange Commission (SEC)

OCIE stated in its 2019 Examination Priorities letter that it “will continue to prioritize cybersecurity in each of its five examination programs. Examinations will focus on, among other things, proper configuration of network storage devices, information security governance generally, and policies and procedures. Specific to investment advisers, OCIE will emphasize cybersecurity practices at investment advisers with multiple branch offices, including those that have recently merged with other investment advisers, and continue to focus on, among other areas, governance and risk assessment, access rights and controls, data loss prevention, vendor management, training, and incident response.”[14]

As it relates to vendor management, areas that the OCIE has stated it will review include:

- Vendor Management Policies and Procedures: Maintain firm policies and procedures related to third-party vendors, such as those addressing the following:
  - Due diligence regarding vendor selection;
  - Contracts, agreements, and the related approval process;
  - Supervision, monitoring, tracking, and access control; and
  - Any risk assessments, risk management, and performance measurements and reports required of vendors.
- Third-party Access: Maintain information regarding third-party vendors with access to the firm’s network or data, including the services provided and contractual terms related to accessing your firm networks or data.
- Third-party Risk Contingency Planning: Maintain information regarding written contingency plans the firm has with its vendors concerning, for instance, conflicts of interest, bankruptcy, or other issues that might put the vendor out of business or in financial difficulty.

On September 26, 2018, the U.S. Securities and Exchange Commission (“SEC”) announced that Voya Financial Advisors Inc. (“VFA”), a Des Moines-based broker dealer and investment advisor, agreed to pay $1 million to settle charges related to an April 2016 data breach that gave unauthorized access to the personally identifiable information of at least 5,600 VFA customers. Even though this is the first SEC enforcement action under the Identity Theft Red Flags Rule, and just the third involving the Safeguards Rule (the previous two actions were brought in 2014 and 2016,

[13] *See* Notice to Members 05-48 for further information about firms’ obligations in outsourcing arrangements.
[14] See OCIE 2019 Examinations Letter

respectively[15]), SEC scrutiny of broker dealer and investment advisor cybersecurity has long been on the horizon. In September 2017, the SEC announced the creation of a Cyber Unit within the Enforcement Division in order to police cyber-related misconduct. In February of 2018, the SEC issued new guidance to public companies on how to disclose cybersecurity risks and incidents to investors. In April 2018, the SEC settled claims with Altaba Inc. (formerly Yahoo! Inc.) in the amount of $35 million in connection with Yahoo's failure to timely disclose a 2014 data breach of hundreds of millions of user accounts. This action is consistent with the SEC's increased focus on cybersecurity and serves as a reminder to companies that the SEC will likely continue to pursue actions under the Safeguards Rule and Identity Theft Red Flags Rule[16]. Additionally, it is possible that the SEC will find software firms held more accountable for the mishandling of a breach.

New York Department of Financial Services (NY-DFS)

The NY-DFS Cybersecurity Regulation (23 NYCRR 500) is a set of regulations from the New York Department of Financial Services that places new cybersecurity requirements on financial institutions. It is generally viewed as one of the most prescriptive sets of law in the area of cybersecurity. The NY-DFS Cybersecurity Regulation applies to all entities (aka, a Covered Entity) operating under NY-DFS licensure, registration, charter, or those that are otherwise DFS regulated. Some broker dealers have chosen to follow it, while others have not. The regulation also applies to unregulated third-party service providers working with those regulated entities.

Section 500.11, Third-Party Service Provider Security Policy, of the law states:

a. Third-party Service Provider Policy. Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third-party Service Providers. Such policies and procedures shall be based on the Risk Assessment of the Covered Entity and shall address to the extent applicable:
    (1) the identification and risk assessment of Third-Party Service Providers;
    (2) minimum cybersecurity practices required to be met by such Third-Party Service Providers for them to do business with the Covered Entity;
    (3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third-Party Service Providers; and
    (4) periodic assessment of such Third-Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices.

b. Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to Third-Party Service Providers including to the extent applicable guidelines addressing:
    (1) the Third-Party Service Provider's policies and procedures for access controls, including its use of Multi-Factor Authentication as required by section 500.12 of this Part[17], to limit access to relevant Information Systems and Nonpublic Information;

[15] Source: SEC, The SEC levied a $75,000 penalty against St. Louis-based broker dealer R.T. Jones Capital Equities Inc. after hackers stole 100,000 individuals' details from its webserver, and subsequently fined Morgan Stanley $1 million after hackers stole client information; September 2015

[16] Source: Alto Litigation, Broker Dealer and Investment Advisor Settles Charges with SEC Related to 2016 Data Breach, October 10, 2018

[17] Section 500.12 Multi-Factor Authentication states, "Multi-Factor Authentication. (a) Based on its Risk Assessment, each Covered Entity shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to Nonpublic Information or Information Systems. (b) Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls."

(2) the Third-Party Service Provider's policies and procedures for use of encryption as required by section 500.15 of this Part[18] to protect Nonpublic Information in transit and at rest;

(3) notice to be provided to the Covered Entity in the event of a Cybersecurity Event directly impacting the Covered Entity's Information Systems or the Covered Entity's Nonpublic Information being held by the Third-Party Service Provider; and

(4) representations and warranties addressing the Third-Party Service Provider's cybersecurity policies and procedures that relate to the security of the Covered Entity's Information Systems or Nonpublic Information.

c. Limited Exception. An agent, employee, representative or designee of a Covered Entity who is itself a Covered Entity need not develop its own Third-party Information Security Policy pursuant to this section if the agent, employee, representative or designee follows the policy of the Covered Entity that is required to comply with this Part.

[18] Section 500.15 Encryption of Nonpublic Information states, "(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. (1) To the extent a Covered Entity determines that encryption of Nonpublic Information in transit over external networks is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO. (2) To the extent a Covered Entity determines that encryption of Nonpublic Information at rest is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.

Additional Legal & Regulatory Resources

FINRA's Report on Cybersecurity Practices (February 2015)

FINRA published a Report on Cybersecurity Practices in the broker dealer industry to highlight effective practices that firms should consider in strengthening their cybersecurity programs. Given the evolving nature, increasing frequency and sophistication of cybersecurity attacks, as well as the potential for harm to investors, firms and the markets, cybersecurity practices remain a key focus for FINRA. FINRA's goal in publishing the report was to focus firms on a risk management-based approach to cybersecurity that is adaptable and capable of addressing evolving threats.

FINRA Report on Selected Cybersecurity Practices (December 2018)

This report continues FINRA's efforts to share information that can help broker dealer firms further develop their cybersecurity programs. Firms routinely identify cybersecurity as one of their primary operational risks. Similarly, FINRA continues to see problematic cybersecurity practices in its examination and risk monitoring program. This report presents FINRA's observations regarding effective practices that firms have implemented to address selected cybersecurity risks while recognizing that there is no one-size-fits-all approach to cybersecurity

OCIE Cybersecurity Examination Sweep Summary (February 2015)

This Risk Alert provides summary observations from OCIE's examinations of registered broker dealers and investment advisers, conducted under the Cybersecurity Examination Initiative, announced April 15, 2014.

New York State Department of Financial Services - Cybersecurity Requirements for Financial Services Companies

The NYDFS Cybersecurity Regulation (23 NYCRR 500) is a set of regulations from the New York Department of Financial Services that places new cybersecurity requirements on financial institutions. This regulation imposes strict cybersecurity rules on covered organizations, such as banks, mortgage companies, and insurance firms. The regulation requires financial companies to install a detailed cybersecurity plan, enact a comprehensive cybersecurity policy, and initiate and maintain an ongoing reporting system for cybersecurity events. The NYDFS Cybersecurity Regulation applies to all entities operating under DFS licensure, registration, charter, or those that are otherwise DFS regulated. The regulation also applies to unregulated third-party service providers working with regulated entities.

California Consumer Privacy Act of 2018

The intentions of the Act are to provide California residents with the right to: 1) Know what personal data is being collected about them; 2) Know whether their personal data is sold or disclosed and to whom; 3) Say no to the sale of personal data; 4) Access their personal data; 5) Equal service and price, even if they exercise their privacy rights.

The CCPA applies to any business, including any for-profit entity that collects consumers' personal data, which does business in California, and satisfies at least one of the following thresholds: 1) Has annual gross revenues in excess of $25 million; 2) Possesses the personal information of 50,000 or more consumers, households, or devices; or 3) Earns more than half of its annual revenue from selling consumers' personal information

2018 Reform of EU Data Protection Rules

As of May 2018, with the entry into application of the General Data Protection Regulation, there is one set of data protection rules for all companies operating in the EU, wherever they are based. Stronger rules on data protection mean: 1) people have more control over their personal data and 2) businesses benefit from a level playing field.

Cybersecurity Standards & Frameworks

NIST Cybersecurity Framework

This voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

SSAE 18 / SOC Reports

Some organizations have heard of SAS 70, SSAE 16, and now SSAE 18, but, haven't seen the value, other than because one of their customers require it. Many companies will not even think about outsourcing functions to a Company who does not have a clean SOC 1 or SOC 2 Type II Report in place, especially since Vendor Management reviews are now required. SOC Reports are created under AICPA guidelines by trained auditors. SOC 2 Type II Reports require a summary of controls reasonably designed to protect confidential data and the testing of the control's effectiveness over an extended period. As of the latest SSAE 18 and SOC 2 updates, vendor management and review of any relevant compliance / audit reports (SOC 1, SOC 2, HITRUST, ISO 27001/2, PCI, etc.) has become a key component of monitoring for potential security and compliance risks when outsourcing functions that use a third-party's data.

ISO / IEC 27000

A set of standards and principles for creating an Information Security Management System (ISMS). It is similar to other ISO standards such as ISO 9000, but focused on those used to manage information security risks and controls within an organization. Bringing information security deliberately under overt management control is a central principle throughout the ISO/IEC 27000 standards.

PCI Security Standards Council

The PCI Security Standards Council is a global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection. The Payment Card Industry Security Standards Council was originally formed by American Express, Discover Financial Services, JCB International, MasterCard and Visa Inc. on 7 September 2006, with the goal of managing the ongoing evolution of the Payment Card Industry Data Security Standard. Such standards are often related to protecting money movement transactions.

cleverDome

cleverDome, Inc. TM is an Arizona Benefit Corporation (B Corporation) that operates as a Co-Op with Members including software service vendors, custodians, broker/dealers, registered investment advisers, financial advisers and ultimately their investor clients (cleverDome Members).

cleverDome has created the first community built and proven model that redefines the standards for protecting the most confidential data and information of consumers in the cloud. cleverDome protects critical data by providing a path forward to take financial services data "under the Dome", i.e. secure and off the open internet

Selected Common Vendor Due Diligence Questionnaires

Center for Internet Security (CIS) — CIS Critical Security Controls (CIS First 5 / CIS Top 20)

The Center for Internet Security (CIS) is a non-profit entity focused on Information Security. According to CIS, its 20 'Controls' are a prioritized set of actions that protect your critical systems and data from the most pervasive cyber-attacks. The First 5 CIS Controls are often referred to as providing cybersecurity "hygiene," and studies show that implementation of the First 5 CIS Controls provides an effective defense against the most common cyber-attacks (~85% of attacks). The CIS Controls map to most major compliance frameworks such as the NIST Cybersecurity Framework, NIST 800–53, ISO 27000 series and regulations such as PCI DSS, HIPAA, NERC CIP (Critical Infrastructure Project), and Federal Information Security Management Act (FISMA).

Cloud Security Alliance — Consensus Assessments Initiative Questionnaire (CAIQ)

The CAIQ provides industry-accepted ways to document what security controls exist in IaaS, PaaS and SaaS offerings. The questionnaire provides a set of questions a reviewer may wish to ask of a cloud provider. The CAIQ questionnaire is designed to support organizations when interacting with cloud provider during the cloud provider assessment process by giving organizations specific questions to ask about provider operations and processes. Sharing the data/CAIQ results is done through the CSA's online registry for security controls, the Security, Trust and Assurance Registry (STAR), using STARWatch, a software-as-a-service application developed by the CSA. The application gives organizations a centralized way to manage and maintain the integrity of the vendor review and assessment process.

Vendor Security Alliance Questionnaire

The Vendor Security Alliance (VSA) is a coalition of companies committed to improving Internet security. The VSA was formed to solve these issues and streamline vendor security compliance. In collaboration with the VSA, top security experts and experienced compliance officers will release a yearly questionnaire to benchmark their risk. Companies can leverage this questionnaire to qualify vendors and ensure the appropriate controls are in place to improve security for everyone. The VSA is organized as a non-profit organization. The first questionnaire was released on October 1st, 2016. The most recent questionnaire was released in January 2019 and is available at: Vendor Security Alliance Questionnaire.

Shared Assessments Standardized Information Gathering (SIG) Questionnaire

The Shared Assessments Program is a membership organization that aims to help companies better manage third-party risk, using controls for cybersecurity, IT, privacy data security and business resiliency. The SIG, developed by Shared Assessments, stands for "Standard Information Gathering", and is a holistic tool for risk management assessments of cybersecurity, IT, privacy, data security and business resiliency in an information technology environment. Unlike some of the other assessments, the SIG evaluates vendors based on its own 18 individual "risk controls". The SIG assessment works to gather pertinent information to determine how security risks are managed across a spectrum of those 18 risk control areas, or "domains", within a vendor's environment, as it calls them.