



A Comprehensive Guide to RIA Compliance

A Guide to Compliance for New Advisors

What You Need to Know to Ensure Your New Registered Investment
Adviser (RIA) Firm Meets Compliance Requirements

Making the move from the wire house or independent broker-dealer to life as an independent Registered Investment Adviser is an exciting prospect. But, it's a process that is also fairly complex. In this article, we will provide a broad overview of what you need to know to make sure your new RIA firm is fully compliant with all the relevant authorities.

No matter how far along you are in the process, these are the top 7 considerations you should make along the way.

1. Draft the Form Filings & Documents You Need in Order to Register Your RIA

In order to register your registered investment adviser ("RIA") firm with the proper authorities, you'll want to make sure you have your forms and filings in order. While not all of the forms we'll review here are *required* upfront (most are, but as always, there are exceptions and exemptions), authorities will expect to see them if and when they [audit your firm](#).

The Form ADV is made up of five parts:

1. Part 1A asks a lot of "who" questions, primarily centered around the owners and advisors at your firm. This section is required whether you are registering with the SEC or the state.
2. Part 1B is only required if you are registering with state authorities, not the SEC.
3. Part 2A requires you to write a narrative brochure where you'll lay out information about your firm's processes, services, fees, etc. This is required when registering with the SEC, unless you are an [exempt reporting advisor](#).
4. Part 2B contains supplemental information about anyone providing financial advice at your firm, including education, business background, conflicts of interest, and disciplinary information.
5. Part 3, better known as "Form CRS," was added in the spring of 2020. It is required for firms registering with the SEC that serve retail investors. In short, the Form CRS is a non-technical document intended for clients that must contain [five sections](#).

[Need help creating your Form CRS? Click here to see how RIA in a Box can help.](#)

For more information on the Form ADV, check out the SEC's [General Instructions and Glossary for the Form ADV](#).

An important note: The number one most common registration deficiency found by the North American Securities Administrators Association (NASAA) [during recent audits](#) was mismatched Form ADV sections. Review your firm's Form ADV regularly to [ensure consistency](#).

Policies & Procedures Manual

In November 2020, NASAA adopted a [new model rule](#) that clarified the essential policies and procedures documents an RIA firm must have. According to the new rule, investment advisors must provide the following:

1. **Compliance Policies and Procedures:** RIAs must establish, maintain, and enforce written compliance policies and procedures reasonably designed to prevent violations by the RIA of the [Uniform Securities Act of 1956](#) and the rules that the securities administrator has adopted under the Act.

2. **Supervisory Policies and Procedures:** RIAs must establish, maintain, and enforce written supervisory policies and procedures reasonably designed to prevent violations by the RIA's supervised persons of the Uniform Securities Act of 1956 and the rules that the securities administrator has adopted under the Act.
3. **Proxy Voting Policies and Procedures:** If an RIA has the authority to vote client securities, then they must explain the process follow the written policies and procedures. If the firm does not have the authority to vote on client securities, then this information must be disclosed to clients.
4. **Physical Security and Cybersecurity Policies and Procedures:** RIAs must establish, implement, update, and enforce written physical security and cybersecurity policies and procedures reasonably designed to ensure the confidentiality, integrity, and availability of physical and electronic records and information. The policies and procedures must be tailored to the RIA's business model, taking into account the size of the firm, types of services provided, and number of locations.
5. **Code of Ethics:** RIAs must establish, maintain, and enforce a written code of ethics that outlines how employees are expected to conduct business, as well as the course of action if an employee violates the Code of Ethics.
6. **Material Non-Public Information Policy and Procedures:** RIAs must establish, maintain, and enforce written policies and procedures reasonably designed to prevent the misuse of material, non-public information by the RIA or any person associated with the firm.
7. **Business Continuity and Succession Plan:** RIAs must establish, maintain, and enforce written policies and procedures relating to business continuity and succession planning.

Investment Advisory Contracts

It is important that you consider how you will create and maintain investment advisory agreements. While this is not submitted as part of an SEC RIA application, most states will examine your form client contracts as part of the registration process. In previous years, NASAA found upwards of [44% of firms](#) audited had at least one deficiency in client agreements.

In order to help keep your contracts in order, consider the following questions:

1. Does your firm have a properly executed, written client agreement on file for each client relationship?
2. Does the fee, formula for calculating the fee, and frequency match how the client is billed?
3. Are your firm's current services provided and/or discretionary authority properly outlined in the executed agreement?
4. Does the contract include any hedge clauses that may stand in conflict with your firm's fiduciary responsibility?

Investment Adviser Representative (IAR) Licensing Requirements

If you're starting your own RIA, chances are you already hold a Series 7, 65, or 66 license (or [one of the professional designations accepted in lieu of them](#)). Now is a good time to make sure everything is up to date and meets the requirements of the authorities you will be registering with.

2. Register Your RIA with the Proper Authorities

Once you have your forms in order, you are ready to register. Depending on a few different factors outlined below, you will need to register your RIA at either the SEC or state jurisdiction level.

When to Register with the SEC

While there are some exceptions, in general, advisers who start an RIA firm with at least \$100 million in assets under management (AUM) must register with the SEC as an RIA.

Some of the more common exceptions that allow investment advisor with less than \$100 million in AUM to register with the SEC include:

- Advisory firms with principal office and place of business in New York generally must register with the SEC if their AUM is \$25 million or greater
- Firms that serve as adviser to an investment company registered under the Investment Company Act of 1940 must register with the SEC regardless of AUM
- RIAs that are *required* to [register in 15 or more states](#) will generally register with the SEC regardless of AUM
- [Internet-only investment advisers](#) may register with the SEC regardless of AUM

For a deeper dive, refer to the SEC's definitive document on the subject, "[Regulation of Investment Advisers by the U.S. Securities & Exchange Commission.](#)"

When to Register with the State

Exceptions aside, prospective RIA firms with less than \$100 million in AUM must register with the relevant state(s), not the SEC. Generally, the advisory firm must register in any state where it:

- has a physical location or office;
- has a representative physically located;
- has five or more clients (or a single client in the states of Texas and Louisiana); or
- is physically soliciting in that state.

That being said, registration processes vary from state to state, and there are some exceptions to these general guidelines. To see each state's RIA registration requirements, check out our [Investment Advisor State Registration Directory](#).

You may be asking yourself, "Does my RIA have to register with FINRA?" The short answer is no. FINRA does not have regulatory authority over RIAs, but it does administer the online filing system for the registration of RIAs and their IARs.

For firm's transitioning from state to SEC registration, you learn more about the most common topics and questions adviser's ask about regulatory compliance during the transition process in [this blog post](#).

RIA State to SEC Registration Transition Checklist

Learn the difference between state and SEC registration and filings.

[DOWNLOAD HERE](#)

3. Choose a Chief Compliance Officer (CCO)

As RIA compliance consultants, we are often asked, "Does my firm need to hire a *dedicated* CCO?" The answer, like many things in the world of RIA compliance, is "it depends."

According to the most recent industry data, a full-time CCO's annual salary could be anywhere between [\\$82,000 and \\$226,000](#). It's easy to understand why only about [3% of firms with less than \\$100 million AUM](#) employ a designated full-time CCO.

RIAs of all sizes are required to have an in-house CCO, but it can be someone who handles other duties. In many cases, the adviser-owner maintains that role in the beginning stage of an RIA's life. This comes with a big pro and a big con.

Pro: You save the money you would have to spend on hiring a full-time CCO.

Con: Your CCO is not very well-versed in RIA compliance.

Partner with an Outsourced Compliance Consultant

Compliance consultants can supplement and assist an RIA's CCO for [a fraction of the cost of hiring an in-person](#) CCO, and quality consultants already have the compliance expertise needed to keep your firm compliant. Even with an outsourced consultant, however, the ultimate responsibility to fulfill your firm's compliance responsibilities ultimately lies in the hands of your designated CCO.

But the good news is that the right compliance consultant can greatly simplify your compliance responsibilities. They improve efficiency and allow you to sleep easier at night knowing your firm is compliant and staying up to date on the latest changes in regulatory rules. Furthermore, a compliance consultant is an invaluable partner if you have concerns or questions about complex regulatory requirements and the actions your firm may need to take. Consider pairing a compliance consultant with compliance technology to enhance your compliance program and overall operational efficiencies.

Pair Compliance Technology with a Compliance Consultant

Adopting a compliance technology solution can save a busy CCO or adviser-owner time. By implementing the right compliance technology, CCOs can gain access to necessary tools to support and create a culture of compliance. The right compliance technology solution can reduce the amount of time spent planning, completing, and documenting regulatory activities by streamlining and simplifying the processes. Pairing compliance technology with a compliance consultant can empower RIAs and their CCOs to navigate the increasingly complex regulatory requirements more efficiently.

[Click here to learn more about how RIA in a Box can help you fulfill your duty as CCO](#)

4. Protect Your RIA Firm from Cybersecurity Threats

Phishing scams, malware, ransomware, trojans—the list of potential avenues for hackers to access your information seems to grow by the minute. As digital becomes a more and more essential part of running an RIA, the realm of cybersecurity presents increasingly dangerous threats to keeping your firm and your clients safe.

Protecting your firm from these threats isn't just a best practice anymore. If, after being hacked, you are found to have not implemented basic protections against such an attack, you could be subject to considerable fines. Do you process online payments? Do you collect personally identifiable information (PII) or hold client financial records? Even if you just use technology in support of basic operations, you are still at risk of ransomware attacks. It's important to consider your specific business practices in order to determine what could potentially be exposed—and how you can protect your firm.

[Click here to download our free Cybersecurity RIA Compliance Checklist](#)

In a 2015 Cybersecurity Examination Initiative, the SEC outlined [six cybersecurity factors](#) for RIAs to focus on:

1. Governance and risk assessment
2. Access Rights and Controls
3. Data Loss Prevention
4. Vendor Management
5. Training
6. Incident Response

Most RIA firms don't have the budget (or need) to hire a full-time Chief Information Security Officer (CISO) or other I.T. personnel to maintain their compliance in every one of these areas. One cost-effective alternative is subscribing to a [cybersecurity platform](#) built to meet all six of the above focus areas.

Another increasingly popular protection in this area is cybersecurity insurance, which we'll discuss in the next section.



5. Get the Right Insurance for Your RIA Firm

While insurance is not a requirement of starting a new RIA firm, there are two types that most RIA firms should at least consider.

Errors and Omissions Insurance

We highly recommend liability insurance to safeguard your firm. Failing to get such a policy leaves your firm vulnerable to a very serious business risk.

Keep in mind though, even the best [E&O insurance plan](#) won't cover an inadequate RIA compliance program. For example, regulatory fines and sanctions will generally not be covered by insurance programs. It's critical that your firm implement internal compliance policies and procedures to establish the proper culture of compliance.

Cybersecurity Insurance

Cyber insurance offers an important, often underrated service to RIA firms. In the case of a cyber attack, many small-to-midsize businesses are at risk of devastating consequences without the [proper cyber coverage](#) in place.

When [selecting cybersecurity insurance](#), it's important that you follow the steps you would follow when choosing any other type of insurance—namely, educating yourself, weighing the options and turning to the experts if you need help.

6. Understand the Fiduciary Duties of an RIA

Fulfilling the role of a fiduciary is a core pillar of the services RIAs provide, so it's important that you understand what that means.

In 2018, the SEC released a document that outlined their views on the fiduciary duties of an RIA, breaking them out into five categories.

1. Duty of Care

The duty of care includes, among other things:

- The duty to act and to provide advice that is in the best interest of the client,
- The duty to seek best execution of a client's transactions where the adviser has the responsibility to select broker-dealers to execute client trades, and
- The duty to provide advice and monitoring over the course of the relationship.

2. Duty to Provide Advice that is in the Client's Best Interest

An RIA's fiduciary duty does not necessarily require the firm to recommend the lowest cost investment product or strategy. That said, it is difficult to argue that a security recommendation is in the best interest of a client if it is higher cost than a security that is otherwise identical (including any special or unusual features, liquidity, risks and potential benefits, volatility and likely performance).

For example, if an RIA advises its clients to invest in a [mutual fund share class that is more expensive than other available options](#), the firm may be violating its fiduciary duty and the antifraud provisions of the Advisers Act. This is particularly true if when the RIA or its personnel are receiving compensation that creates a potential conflict and if the firm does not, at a minimum, provide full and fair disclosure of the conflict, describe its impact on the client, and obtain informed client consent regarding the conflict.

3. Duty to Seek Best Execution

When [seeking best execution](#), an RIA should consider “the full range and quality of a broker's services in placing brokerage including, among other things, the value of research provided as well

as execution capability, commission rate, financial responsibility, and responsiveness” to the investment adviser.

In other words, the determinative factor is not the lowest possible commission cost but whether the transaction represents the best qualitative execution. Further, an investment adviser should “periodically and systematically” evaluate the execution it is receiving for clients.

4. Duty to Act and Provide Advice and Monitoring over the Course of the Relationship

An RIA is required to provide advice and services to a client over the course of their relationship at a frequency that is both in the best interest of the client and consistent with the scope of advisory services agreed upon between the investment adviser and the client.

The duty to provide advice and monitoring is particularly important for an adviser that has an ongoing relationship with a client (for example, a common relationship where the adviser is compensated with a periodic asset-based fee or an adviser with discretionary authority over client assets).

5. Duty of Loyalty

An RIA must seek to avoid conflicts of interest with clients, and, at a minimum, make full and fair disclosure to clients of all material conflicts of interest that could affect the advisory relationship. However, disclosure of a conflict alone is not always sufficient to satisfy the adviser’s duty of loyalty and Section 206 of the Advisers Act.

Any disclosure must be clear and detailed enough for a client to make a reasonably informed decision to consent to such conflicts and practices or reject them. An investment adviser must provide the client with sufficiently specific facts so that the client is able to understand the adviser’s conflicts of interest and business practices well enough to make an informed decision. For example, an RIA disclosing that it “may” have a conflict is typically not adequate disclosure when the conflict actually exists.

7. Properly Address Disciplinary Disclosures

The SEC has stated in no uncertain terms that [it pays extra attention to firms where individuals with disciplinary disclosures work](#). If you or someone you work with has a disclosure on their record, there are a few important items to keep in mind.

You *Must* Disclose Them

This might seem obvious when discussing something called “disclosures,” but the [SEC regularly audits firms](#) only to find they:

1. Omitted material disclosures regarding disciplinary histories of certain supervised persons or the adviser itself.
2. Included incomplete, confusing, or misleading information regarding disciplinary events.
3. Did not timely update and deliver disclosure documents to clients, such as updating Form ADV for new disciplinary events of supervised persons reported on CRD (e.g., Form U5s).

You Must Address the Risks

If you or someone on your team has disclosures, your policies and procedures need to demonstrate that you understand the risk. The SEC found that [many firms had not done so](#).

From a 2019 SEC risk alert:

Advisers did not have processes reasonably designed to identify:

1) Whether the supervised persons' self-attestations regarding disciplinary events completely and accurately described those events. For example, some self-attestations contained information that did not fully or clearly describe the disciplinary events.

2) Whether the supervised persons' self-attestations that they were not the subject of reportable events or recent bankruptcies was in fact the case. For example, some supervised persons reported incorrectly to the adviser that they were not the subject of any reportable events during the reporting period or did not report information regarding recent bankruptcies.

There you have it — the basic steps for starting a compliant RIA firm:

1. Get the required forms and filings
2. Register with the proper authorities
3. Choose a CCO
4. Address cybersecurity threats
5. Make sure you have the right insurance
6. Understand the fiduciary duties of an RIA
7. Properly address disciplinary disclosures

[Want to discuss your situation with a compliance professional? Click here to contact RIA in a Box](#)