



# AdvisorDefense

(406) 686-3086

[www.advisordefense.com](http://www.advisordefense.com)

[sales@advisordefense.com](mailto:sales@advisordefense.com)







AdvisorDefense, LLC All rights reserved.

# Why **Advisor**Defense?



As fiduciaries, Registered Investment Advisers (RIAs) have an ongoing obligation to prioritize their clients' best interests, encompassing the safeguarding of client data and shielding them from cyber threats. Reinforcing this commitment, the U.S. Securities and Exchange Commission's (SEC's) latest regulations on cybersecurity risk management went into effect on **December 18th, 2023**, primarily targeting publicly listed firms. Nevertheless, anticipated rules tailored for investment advisors are projected to be ratified in 2024.

Our **AdvisorDefense** service provisions have been meticulously crafted to align with the SEC's key requirements, ensuring compliance while maintaining minimal disruption for our valued clients.

| Key Requirements  | Description  |
|---|--|
|   | <b>Cybersecurity Risk Management</b><br>Adopt and implement written cybersecurity policies and procedures designed to address cybersecurity risks                                |
|  | <b>Cybersecurity Strategy</b><br>A plan of action designed to maximize the security and resiliency of your firm  |
|  | <b>Cybersecurity Governance</b><br>Annual reporting to the owners and/or executive management persons  |
|  | <b>Vendor Due Diligence</b><br>Ensure client information is protected by third-party vendors engaged by an RIA   |
|  | <b>Material Cybersecurity Incident Disclosure</b><br>Report material cybersecurity incidents within four business days following the determination of the incident's materiality |

The framework allows RIAs to engage **third-party cybersecurity experts**, offering diverse viewpoints and specialized expertise in comprehending and aiding in risk management.

**The time to comply is NOW!**  
***Protect your Clients. Maintain your reputation.***  
***Ensure Compliance.***



# AdvisorDefense

## SEC Adopts Important Rule Amendments to Regulation S-P

---

On May 15th 2024, the U.S. Securities and Exchange Commission adopted amendments to Regulation S-P, which requires registered investment Advisors (RIAs) to adopt written policies and procedures to safeguard customer records and information (the “safeguards rule”).

These amendments aim to enhance the policies and procedures of RIA’s regarding the protection of client sensitive information, especially policies on incident response, client notification, disposal of client sensitive information, and service provider due diligence.

### **Compliance Date**

Mandatory compliance, 60 days after posting on the federal registrar, Advisors have the following timeline to comply with the amendment:

- Advisors with at least \$1.5 billion or more in AUM: **18 Months**
- Advisors with less than \$1.5 billion in AUM: **24 Months**

### **Enhancements to Regulation S-P**

***Incident Response Program*** - The amendment requires that Advisors adopt policies and procedures that are reasonably designed to detect, respond to, and recover from unauthorized access to, or use of, client data. Further, these policies must include the following:

- **Assessment:** Advisors will evaluate the nature and scope of the breach and/or incident;
- **Containment:** Implement remedial measures to prevent further incidents and/or unauthorized access; and
- **Notification:** Policies must be in place to notify affected clients as soon as possible, but no later than 30 days after detection of the incident and/or breach, and ensure proper information is disclosed to the client.



# AdvisorDefense

## SEC Adopts Important Rule Amendments to Regulation S-P

---

***Service Provider Oversight*** - RIAs must implement policies and procedures designed to oversee Service Providers, through due diligence on and ongoing monitoring. The amendment defines “Service Provider” as any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a covered institution. RIAs must ensure that Service Providers have controls in place to protect against unauthorized access to, or use of, client information. Service Providers must provide notification to Advisors regarding unauthorized access to client information, ASAP, but no later than 72 hours after becoming aware of the breach.

***Customer Notification Requirement*** - RIAs must notify affected individuals promptly when sensitive customer information was, or is reasonably likely to have been, accessed or used without authorization. Notices must include:

- Comprehensive details about the incident.
- Specifics on the type of data that was breached.
- Instructions for affected individuals on how to address the breach and protect themselves.

An exception to the customer notification requirements exists when an RIA can evidence that sensitive customer information has not been, and is not reasonably likely to be, used in a manner that would result in substantial harm or inconvenience.

# Our Mission



Our mission is to be the vanguard of cybersecurity excellence, ensuring that organizations, regardless of size or resources, receive unparalleled protection. We firmly believe that every Registered Investment Advisor (RIA) should have access to state-of-the-art cybersecurity solutions that bolster their digital fortitude in an era rife with potentially catastrophic cyber threats.

Recognizing the challenges faced by RIAs in employing dedicated Chief Information Security Officers and Chief Technology Officers, we stand as a steadfast guardian, providing the essential tools, expertise, and strategies needed to navigate and withstand the constantly evolving landscape of cyber risks.

**AdvisorDefense** is committed to empowering RIAs with the comprehensive defense necessary to safeguard their operations and clients from the perilous consequences of cyber attacks and to comply with industry regulations.

## *Competitive Advantages and Market Differentiation*



### **Tailored Approach**

Our commitment to tailoring services to each client's unique environment ensures that organizations receive targeted, relevant assessments that directly address their vulnerabilities.



### **Expertise**

Our team comprises cybersecurity veterans with a deep understanding of evolving threats and countermeasures. This expertise enables us to deliver insights that organizations can trust and act upon.



### **Actionable Insights**

We don't stop at identifying vulnerabilities; we provide actionable recommendations for remediation. This practical approach equips clients with clear strategies to bolster their defenses.



### **Partnership**

We view our clients as partners, collaborating closely to ensure that our services align with their business objectives and risk tolerance. This collaborative spirit fosters lasting relationships built on mutual trust.



### **Innovation**

Our commitment to staying ahead of the curve allows us to embrace emerging technologies and methodologies, ensuring that our clients receive the most effective and up-to-date solutions.

# Our Value Proposition

---



Our offering will be led by an experienced real-world CISO and CTO with over two decades of experience in the financial services sector.



Wealth of Expertise  
(over two decades)



Features in publications  
including *Financial Planning* and *Citywire*.



2023 RIA Intel Awards' Industry  
Advocate of the Year finalist



The support chassis of **AdvisorDefense** includes **AdvisorAssist**, the preeminent consulting firm for RIAs, and **Merchant**, a leading strategic partner for wealth management firms and our industry community at large.



---

The premier solution for cybersecurity and regulatory adherence for the RIA industry, designed by experts from the RIA industry. Solving unique regulatory requirements and cybersecurity challenges for RIAs.

Built on **collaboration**, **innovation**, and **steadfast client dedication**, our approach acknowledges the dynamic nature of cybersecurity. Recognizing its unique challenges, we tailor solutions through a collaborative journey, ensuring your firm's specific needs are met.

---

Our customized audits cater to clients who may not be prepared for an annual commitment with AdvisorDefense, confident in the coverage provided by their IT Provider and internal controls. Firms have the flexibility to opt for an initial assessment or a mock examination. These audits serve a dual role: they fulfill the mandatory testing of an RIA's compliance program effectiveness, as stipulated by Rule 206(4)-7. Additionally, they offer an avenue to acquaint clients with the benefits of collaborating with AdvisorDefense for our continuous services, potentially enhancing their cybersecurity posture and regulatory compliance.

| Initial Assessment                                  | Deliverables   |
|---|--|
| <b>Vulnerability Scan</b>                           | Provide a one-time vulnerability report, utilizing a lightweight agent installed on each endpoint and a probe on your primary office network. Our solution will scan your network to identify vulnerabilities, including missing patches, misconfigured devices, and Common Vulnerabilities and Exposures (CVE). |
| <b>Risk Assessment</b>                              | Conduct a one-time comprehensive risk assessment and gap analysis of your cybersecurity posture. This involves evaluating existing policies, procedures, and technical controls to identify vulnerabilities, risks, and areas for improvement.   |
| <b>Detailed Summary Report With Recommendations</b> | Analyze the results of the scans and provide the Advisor with a detailed report outlining the identified vulnerabilities and recommendations for enhancements to the existing network infrastructure or replacement using <b>AdvisorDefense</b> systems and or tools.  |

| Mock Examination                        | Deliverables   |
|---|--|
| <b>Cybersecurity Posture Evaluation</b> | AdvisorDefense will perform a simulated assessment designed to evaluate your compliance with applicable cybersecurity regulations and standards. This mock exam will involve reviewing policies, procedures, technical controls, and documentation to assess adherence to relevant regulatory frameworks.  |
| <b>Real World Simulation</b>            | Through our mock examination, we simulate real-world regulatory audits, providing a rigorous testing ground to ensure your readiness for any scrutiny from regulatory bodies like the SEC. By mimicking the complexities and nuances of actual assessments, we help you uncover weaknesses and fine-tune your defenses, ultimately fortifying your organization against potential threats and compliance pitfalls. |



# AdvisorDefense

## SERVICE COMPARISON



|  | Essentials    | Advantage     | Advantage Plus |
|--|---------------|---------------|----------------|
| Cybersecurity Risk Assessment  | ✓             | ✓             | ✓              |
| Policies and Procedures Creation & Review (Includes: WISP, IRP, and Vendor Risk Management Policy) | ✓             | ✓             | ✓              |
| Regulatory and Cybersecurity Alerts  | ✓             | ✓             | ✓              |
| Vendor Risk Management Library   | Limited       | Limited       | ✓              |
| Cybersecurity Gap Analysis   | Up to 2 Hours | Up to 4 Hours | ✓              |
| Cybersecurity Strategy Calls   | Annual        | Quarterly     | Monthly        |
| Included Consulting Hours<br><small>Can be applied to any of the services listed below</small>     | Up to 4 Hours | Up to 6 Hours | Up to 12 Hours |
| Microsoft 365 and Google Workspace Technical Assessments   | ✗             | ✗             | ✓              |
| Cybersecurity Regulatory Exam Support  | ✗             | ✗             | ✓              |
| Cybersecurity Breach Response and Remediation Guidance   | ✗             | ✗             | ✓              |
| Virtual Trainings  | ✗             | ✗             | ✓              |
| Mock Incident Response Exercises   | ✗             | ✗             | ✓              |
| Ongoing Managed Service Provider (MSP) Oversight   | ✗             | ✗             | ✓              |

\* Any item marked with an "X" can be added on to a service model for an additional cost.

### Optional Services

Cybersecurity Awareness Training  
 24/7 Managed Detection and Response (MDR)  
 Vulnerability Scanning - Network and Web Application  
 Penetration Testing - Network, Wireless, and Web Application  
 Cybersecurity Regulatory Exam Mock Audits

**Want to Learn More?** Contact us at (406) 686-3086 or [sales@advisordefense.com](mailto:sales@advisordefense.com)





(617) 800-0388

[www.advisordefense.com](http://www.advisordefense.com)

[sales@advisordefense.com](mailto:sales@advisordefense.com)



© AdvisorDefense, LLC All rights reserved.