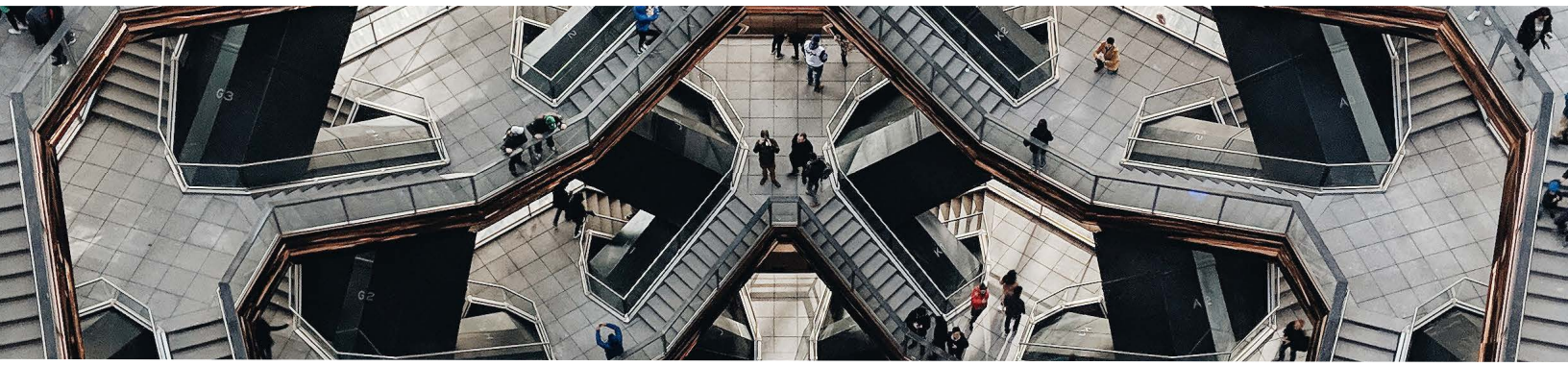
AGIO SEC CYBERSECURITY MOCK AUDIT



As cybersecurity continues to evolve and hackers become more and more sophisticated, the SEC Office of Compliance Inspections and Examinations (OCIE) has prioritized evaluating funds, specifically against the areas of risk cited in multiple Risk Alerts the regulator has released dating back to 2014. "Never before examined" (NBE) funds are at the greatest risk of being audited, with those firms that haven't been examined in the last five to seven years coming in a close second. We say, "it's not a matter of if, but when," when it comes to being breached, and the same holds true for being audited by the SEC – it's not if, but when.

Agio's SEC Cybersecurity Mock Audit is a consulting engagement designed to prepare you for when that day comes. We review your firm's policies, procedures, and workflows in order to identify areas where the SEC may find you deficient. Our engagement prepares your senior management to respond to an actual audit, and effectively communicate to regulators your firm's cybersecurity approach. With our experience as vCISOs who have sat in the boardroom and assisted with actual regulatory audits, we know exactly what it takes to keep you safe and compliant.

THE PROCESS

We specifically review how your firm is addressing the SEC's 28 Areas of Interest, 6 Areas of Focus, and the required Reg S-P administrative, technical, and physical safeguards related to customer/investor non-public personal information and personally identifiable information ("PII"). This is critical, as all three SEC cybersecurity enforcement actions against RIAs have been due to a "failure to safeguard customer/investor data."

From the beginning, we kick off your audit with document reviews prior to the sessions with your team. And your team usually consists of your CTO/IT Director, COO, CFO, HR, General Counsel, Investor Relations, and internal and/or outsourced IT team. Then, over the course of one to two days we evaluate the policies, procedures, workflows, and required privacy/opt-out notices in order to identify areas where your firm may be deficient.

We conclude our engagement by providing you meaningful recommended corrective actions that will enable you to demonstrate compliance with the required safeguards. These recommended corrective actions – i.e. "deficiencies," as the OCIE refers to them – can be both administrative and technical.

Administrative corrective actions in nature are generally addressed in three to six months, while certain technical corrective actions can require more time and planning. It's worth noting that any support our clients need when it comes to technical remediation, Agio can and does assist to accelerate the strengthening of your audit preparation and overall cybersecurity posture.

PRODUCTIVITY, COST & RISK

Our SEC Cybersecurity Mock Audit enables you to easily prioritize your compliance efforts based on those areas most in need of attention. We save you time, energy, and resources because we review the elements of each risk alert and each piece of regulation, consolidate those requirements, and cross-map them – all so you don't have to. And by going through this process now, you'll have time to prepare your firm and develop your artifacts, reducing your effort, cost (and stress level) when you receive the notice of an actual exam. Our resulting report for you also maps required documentation to each control so you are crystal clear for the future exam. Finally, our audit provides us the opportunity to compare what's in place or missing within your firm's overall cybersecurity strategy against what's considered best practice or a best-in-breed solution today. This enables you to see where you can fortify your cybersecurity posture and where you're already strong.

WHY NOW?

For some of our clients, there comes a time when the anxiety or fear of being audited is so great it spurs them into action. For other clients, the impetus comes from investor pressure or C-suite inquiry as to "what we're doing for cyber." No one wants a fine or an OCIE deficiency letter that could damage their reputation and shrink their AUM. When you're ready to tackle the cybersecurity audit head on, we're here and we're ready to help.

WHY AGIO?

#OneAgio

When you select Agio, you're investing in a relationship with everyone who's a part of this firm. Our teams operate in a symbiotic relationship, based on deposits and withdrawals, that creates a vehicle for delivering more than just service. We deliver an experience that reaffirms to our clients we've got them covered. From clean, concise implementations; to consistent support backed by automation and tools that work the way they're supposed to; to value-add reporting; to accurate, timely invoicing; and content on the latest IT and cybersecurity trends, we bring the full breadth and depth of our talent to bear. We deliver #OneAgio.