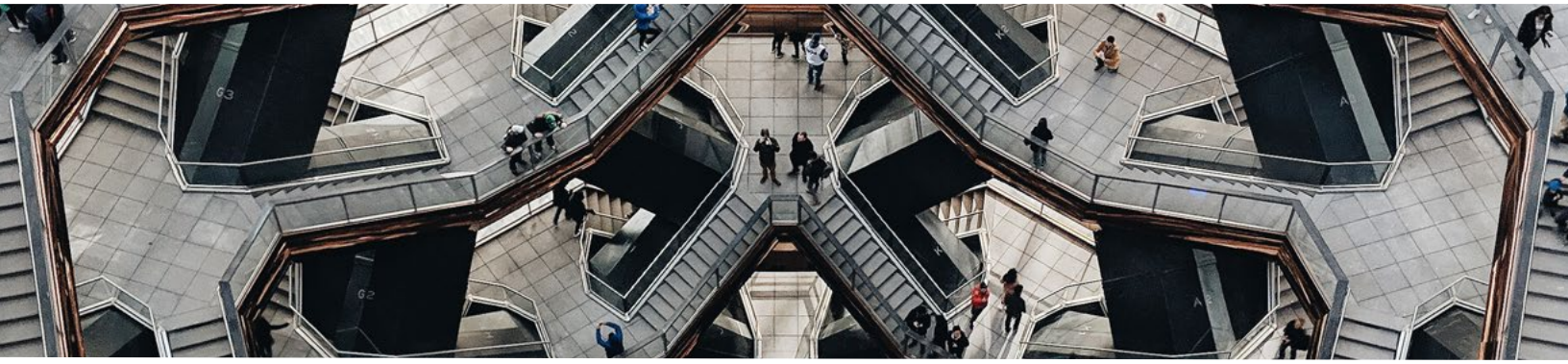
AGIO SEC CYBERSECURITY MOCK AUDIT



With the new SEC Cybersecurity Risk Management Rules, ensuring your firm is cybersecurity compliant can no longer be ignored. The new rules require investment advisers and broker-dealers to have robust cybersecurity policies and procedures in place to safeguard their client's confidential information from cyber threats.

Agio has developed an SEC Cybersecurity Mock Audit program to help you prepare for your next regulatory audit. Our process examines how prepared your firm is to meet requirements covered in the SEC Rules 38a-2 and 206(4)-9 and required Reg S-P administrative, technical, and physical safeguards related to customer/investor non-public personal information and personally identifiable information ("PII").

THE PROCESS

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 to identify areas where your firm may be deficient.

We conclude our engagement by providing you with meaningful recommended corrective actions that will enable you to demonstrate compliance with regulations. These recommended corrective actions – i.e., “deficiencies,” as the SEC 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 for any support our clients need when it comes to technical remediation, Agio can and does assist in accelerating 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 examination from the SEC. Our resulting report maps out for you the required regulatory documentation, so you are equipped to respond quickly and confidently on your next exam. Finally, our audit gives you the opportunity to compare what's in place or missing within your firm's overall cybersecurity strategy against what's considered industry best practice. This enables you to identify where you can fortify your cybersecurity posture and where you're already strong.

WHY NOW?

Cybersecurity regulation is here. The SEC's Cybersecurity Risk Management rules (Rules 38a-2 and 206(4)-9) mean you can no longer afford to delay action. It's become clear through the rulemaking process that the compliance (and reputational) risks of not having the right controls in place will be significant when SEC examiners begin their audits.

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 that 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.