

RIA compliance checklist

Core compliance

- Register with the SEC (if \$100M+ AUM) or state regulator; keep registration current
- Appoint a chief compliance officer (CCO)
- Maintain a code of ethics
- Develop written policies and procedures tailored to your business and client base
- Document how you identify and handle conflicts of interest
- Keep detailed, organized records
- Ensure honest and fair marketing and advertising
- Protect client privacy and safeguard sensitive information
- Oversee service providers and branch offices for compliance

Annual and ongoing

- Update and file Form ADV every year
- Conduct and document a compliance review every year
- Review and update code of ethics every year
- Provide compliance training for all staff every year
- Test/audit compliance systems (spot-check records, run mock audits)
- Review all marketing/advertising for accuracy and compliance
- Update business continuity plan
- Obtain clear client consent for major service or agreement changes
- Assess and update compliance policies and procedures as business or regulations change

Cybersecurity

- Maintain up-to-date cybersecurity policies and procedures
- Protect critical services and client data from cyber threats
- Prepare for disruptions due to cyberattacks
- Train staff to detect, report, and recover from incidents
- Test and review cybersecurity measures
- Assess and manage third-party/vendor cybersecurity risk
- Discourage use of unsupported or shadow IT systems