CENTRL

This 10-point checklist is intended to help prepare RIAs for the proposed new Third Party Risk Management rule under the Investment Advisors Act of 1940.

Third Party Risk Management Checklist for RIAs

- Take a risk-based approach to developing your program. Categorize all vendors by criticality and risk level.
- Identify and document the nature and scope of the services your providers offer. Determine if they are considered a “covered function or service” as defined by the SEC.
- Identify and assess any potential risks resulting from the service provider performing the covered function, including how to mitigate and manage such risks.
- Evaluate the service provider's competence, capacity and resources necessary to perform the covered function.
- Review and assess vendor due diligence questionnaires, business continuity plans and assurance reports from independent parties.
- Where possible, leverage industry standard templates to minimize the burden on vendors and gain internal efficiencies.
- Document and monitor third party operational resiliency and certification attainments.
- Track the implementation of compliance policies, procedures and controls relating to systems.
- Validate vendor self-assessments with objective external evidence and surveillance, especially vendors in the cyber domain.
- Collect results of any stress testing being done to ensure compliance with security controls.
- Conduct periodic onsite visits, annually if possible.