Ready for the SEC Cybersecurity Management Rules?

## Visory's Cybersecurity Readiness Checklist: Does your RIA Check All These Boxes?

The SEC's new cybersecurity rules for advisors are coming. RIAs should take stock of the current state of their cybersecurity now to ensure that their protocols and procedures will comply with the forthcoming rules, particularly around risk management, reporting, disclosures and recordkeeping. Not sure where to begin? Our checklist is a good place to start:

	SECURITY MEASURE	IN PL YES	ACE NO
1.	Written cybersecurity plans, policies and procedures. RIAs need formal cybersecurity risk plans, policies and procedures. This includes written documents that clearly detail workflows and responsibilities.		
	Riskassessment		
	Cybersecurity policy		
	Employee/staff training and testing: Description of the program Evidence of implementation and effectiveness		
2.	<b>Policies and procedures for data access management.</b> The SEC wants firms to have detailed Acceptable Use Policy (AUP) documents in place. Firms need protections like multifactor authentication (MFA), least-privilege access rights and zero-trust monitoring of end devices to comply with the new rules.		
	Acceptable use policy (AUP)		
	Multifactor Authentication (MFA)		
	Access management		
	Classify data		
	Evidence of enforcement		
З.	<b>Protection for data and information.</b> Data must be protected at rest and when in motion. This means relying on things like encryption, threat detection and prevention and mobile device management technologies that can address their vulnerabilities and keep information secure at all times.		
	Data loss prevention measures such as:Perimeter securityPatch managementEncryption (in motion and at rest)Proper disposal of equipmentInventory of hardware and softwareVulnerability scanning		
	Mobile security such as: Mobile device management (MDM) policy 🛸 Bring your own device (BYOD) policy		

	SECURITY MEASURE	IN PL YES	ACE NO
4.	<b>Continuous monitoring.</b> The SEC expects RIAs will continuously monitor for threats and vulnerabilities. Consider integrated platforms that can do just that - monitor, alert, respond to and remediate cybersecurity attacks.		
	Evidence of monitoring such as: failed logons, lockouts, elevations, etc.		
	Vendor due diligence and management		
5.	<b>Incident response planning and recovery.</b> Every RIA will need a documented incident response plan it can point to in the event of a cyberattack. The plan should be tested for effectiveness and speed of recovery, with gaps addressed to assure business continuity in the event of a significant incident, regardless of where the firm's data resides.		
	Business continuity plan		
	Timely detection		
	Corrective actions		
	After action review		
	Cybersecurity insurance		
6.	<b>Reporting and disclosures.</b> RIAs will be on the hook for reporting significant qualifying cyber events to the SEC within a relatively short period of time.		
	Form ADV-C		
	Form AV Part 2A		
7.	<b>Formal accountability.</b> Firms need to establish the internal team accountable for managing cybersecurity risk, addressing cybersecurity threats, and approving cybersecurity policies and procedures. Key point: regardless of whether they outsource cybersecurity, firms are still responsible for that oversight.		
	Active senior level engagement		
	<ul> <li>Vendor management:</li> <li>Due diligence – including how client data is protected</li> <li>Annual oversight and review</li> <li>Business continuance</li> <li>Monitoring and testing</li> <li>Review of written contracts</li> </ul>		

## If you checked NO more than twice, your firm might be at risk. For a risk assessment, call us at 913.396.4600

