VENTURIS SOLUTIONS

RIA Cybersecurity Readiness Checklist

Could your firm detect, respond to, and recover from a cyber incident?

		YES	NO
1	**Written Incident-Response Plan** Current written plan for detecting, containing, responding and recovering; roles, decision-makers, escalation and communication responsibilities identified.	☐	☐
2	**Customer and Regulatory Notification** Documented process for determining notification obligations after an incident; clear ownership for notification decisions and approvals.	☐	☐
3	**Vendor and Service-Provider Oversight** Inventory of vendors accessing sensitive information maintained; vendor cybersecurity practices evaluated with expectations for prompt incident reporting.	☐	☐
4	**Identity and Access Management** MFA required for email, remote access, admin accounts and sensitive systems; access based on role and removed promptly on departure.	☐	☐
5	**Endpoint Protection and Monitoring** Computers and servers protected with managed EDR; security alerts actively reviewed, investigated and resolved.	☐	☐
6	**Centralized Logging and Threat Detection** Security activity collected from endpoints, identity systems, email, firewalls and critical systems; someone reviews alerts and responds to suspicious activity.	☐	☐
7	**Email Security and Employee Awareness** Practical cybersecurity and phishing-awareness training throughout the year; procedures for verifying payment requests and unusual email instructions.	☐	☐
8	**Backup and Recovery** Critical systems backed up regularly using secure, protected backups; periodic testing confirms systems can be restored after an outage or attack.	☐	☐
9	**Vulnerability and Patch Management** Accurate inventory of devices, systems and software; security updates and critical patches installed within defined timeframes and tracked.	☐	☐
10	**Documentation and Testing** Evidence retained for training, vendor reviews, monitoring, incident-response testing and corrective actions; program reviewed and tested regularly.	☐	☐

This checklist is a preliminary self-assessment and is not a certification of cybersecurity or regulatory compliance.

How Did Your Firm Score?

Give your firm one point for each numbered area where you can confidently check both statements.

8–10: Strong foundation
Your firm is well-prepared to detect, respond to, and recover from cyber incidents.

5–7: Important gaps may remain
Your firm has key elements in place, but improvements are needed.

0–4: Immediate attention recommended
Your firm is at higher risk. Take action to address critical gaps.

Turn Your Checklist Into an Action Plan

Schedule an RIA Cybersecurity Readiness Conversation

Paul Mallory

Venturis Solutions

info@venturissolutions.net

www.venturissolutions.com