RIA Cybersecurity & IT Compliance Checklist

This checklist is designed for Registered Investment Advisors (RIAs) to ensure they meet SEC and FINRA cybersecurity and IT compliance expectations. Use it as a quick reference to strengthen your firm's security posture and prepare for regulatory audits

1 Governance & Compliance Oversight

- ☐ Written Information Security Program (WISP) in compliance with SEC Regulation S-P
- ☐ Qualified compliance officer or outsourced equivalent
- ☐ Annual compliance review under the Advisers Act (Rule 206(4)-7)

2 Access Control & Authentication

- ☐ Multi-Factor Authentication (MFA) for all accounts with sensitive data access
- ☐ Role-Based Access Control (RBAC) to limit data access
- ☐ User Account Management Policy for onboarding and offboarding staff

3 Data Protection & Privacy

- ☐ Encryption of data at rest and in transit
- ☐ Data Classification Policy for handling sensitive information
- ☐ Secure Disposal Policy for physical and digital records

4 Cybersecurity Controls

- ☐ Incident Response Plan with breach notification procedures
- ☐ Vendor Risk Management Policy with documented due diligence
- ☐ Patch Management Policy for timely updates

5 Business Continuity & Disaster Recovery

- ☐ Business Continuity Plan (BCP)
- ☐ Disaster Recovery Plan (DRP) with offsite backups
- ☐ Regular testing and updating of BCP/DRP

6 Monitoring & Reporting

- ☐ Security Monitoring Policy with continuous threat detection
- ☐ Annual Cyber Risk Assessment
- ☐ Compliance Reporting Procedures for regulators and clients

7 Employee Awareness & Training

- ☐ Ongoing Security Awareness Training
- ☐ Acceptable Use Policy (AUP) for company systems
- ☐ Regular phishing simulations