Technology Risk Assessment Framework

Advisor firms may be more highly valued when they have a documented understanding of their risks, and strategies for reducing them.

This assessment framework helps firms evaluate technology, cybersecurity, operational resilience, and vendor dependency risks.

It is designed to identify:

- Business continuity vulnerabilities
- Cybersecurity and data protection risks
- Key-person dependencies
- Vendor concentration risks
- Opportunities to strengthen governance and scalability

The objective isn't to bring technology fully in-house, but to determine:

- What the firm must directly control
- What capabilities can be outsourced
- Where redundancy is required
- What investments the firm should prioritize over the next 2–3 years

Simplified Assessment Framework

Step 1: Assess Current Governance & Documentation

Does your firm have a documented:

- Cybersecurity policy?
- Onboarding process for new advisors and employees that includes an introduction to the firm's privacy/cybersecurity/technology policies?
- Business continuity plan?
- Disaster recovery procedure?
- Incident response procedures?
- Vendor management process?

Questions:

- When were these documents last reviewed?
- Who is accountable for maintaining them?
- Have they been tested?

Step 2: Identify Critical Business Systems

Which systems would significantly disrupt the practice if unavailable? Consider those internal business systems for which your firm is responsible or where you have a vendor agreement in place.

Examples:

- CRM
- Financial planning software
- Client portal
- Email
- Phone system
- Document/file management system
- Cybersecurity tools
- Payroll system
- Accounting software
- AI tool(s)

For each system:

- How critical is it?
- Who is accountable for it?
- How long could the firm operate without it?

System	Critical/Important/Nice-to-Have	Who is Accountable?	How Long Could You Go Without It?
CRM	Critical		2 days
Financial planning software	Critical		1 week
Client portal	Important		2 weeks
Email	Critical		4 hours

Step 3: Evaluate Key-Person Risk

Consider the following:

- Is critical knowledge concentrated in one individual?
- Who manages vendors?
- Who understands your systems integrations and workflows?
- Who manages cybersecurity?
- Who administers systems?

For each key dependency:

- What happens if the individual is unavailable?
- Is there backup coverage?
- Is knowledge documented?

Step 4: Evaluate Vendor Dependence

Create a list of critical vendors:

Examples:

- CRM provider
- Managed IT provider
- Cybersecurity provider
- Financial planning software provider
- Phone system provider
- Accounting software provider

Questions:

- How dependent are we on each vendor?
- Are service expectations documented?
- Is performance reviewed?
- Is there an alternative if the vendor fails?

Step 5: Assess Cybersecurity Readiness

Review:

- Multi-factor authentication
- Endpoint protection[1]
- Email security
- Password management
- Security awareness training
- Data backup procedures
- Patch management[2]
- Cyber insurance coverage

[1] Endpoint protection is security software that protects every work device that touches client data, email, CRM, planning software, and other systems your firm uses.

[2] Patch management is the process of regularly updating software, operating systems, and devices to fix security vulnerabilities, improve performance, and reduce the risk of cyberattacks.

Consider the following:

- When was the last security assessment completed?
- Are employees regularly trained?
- Have backups been tested?

Step 6: Define Ownership vs Outsourcing

For each capability, determine whether the firm should:

OWN -- Directly oversee and govern

Examples:

- Technology roadmap
- Cybersecurity accountability
- Vendor governance
- Data governance
- Business continuity planning

PARTNER -- Outsource but actively manage

Examples:

- Managed IT services
- Cybersecurity monitoring
- Application support
- Help desk

BUY -- Purchase as standardized services

Examples:

- CRM
- Financial planning software
- Phone systems

Step 7: Assess Future-State Readiness

- Will your firm's current technology support growth over the next 3 years?
- Can your current systems support additional advisors?
- Can your technology support an acquisition, if that's part of your plan?
- Can your technology support increased compliance requirements?
- Are there emerging AI opportunities you should explore?

Step 8: Develop a 3-Year Roadmap

Prioritize initiatives under:

Immediate (0–12 Months)

Examples:

- Enable MFA firm-wide
- Document critical processes
- Test backup procedures
- Test incident responses processes

Near-Term (1–2 Years)

Examples:

- Improve cybersecurity maturity
- Reduce key-person risk
- Review vendor contracts
- Expand AI capabilities

Long-Term (2–3 Years)

Examples:

- Modernize core systems
- Improve automation
- Enhance client experience
- Strengthen vendor governance

Step 9: Create a Summary

Current-State Assessment

Critical Systems

- _____
- _____

Critical Vendors

- _____
- _____

Key-Person Dependencies

- _____
- _____

Major Risks

- _____
- _____

Future-State Recommendation

Capabilities to Own

- _____

Capabilities on which to Partner

- _____

Capabilities to Buy

- _____

Priority Initiatives (Next 2 Years)

Initiative	Priority: (High/Medium/Low)	Timeline