CRISIS IQ
PARTNERS

CRISIS PLANNING CHECKLIST FOR PROFESSIONAL & FINANCIAL SERVICES

Is Your Firm Ready to Handle a Crisis?

Use this checklist to assess your current crisis preparedness and identify gaps that could expose your firm to regulatory penalties, client losses, or reputational damage.

CRISIS PLANNING ESSENTIALS

Crisis Management Framework

- [ ] Written crisis management plan exists and is current (updated within last 12 months)
- [ ] Crisis team identified with primary and backup members for each role
- [ ] Clear escalation protocols defining when to activate the crisis plan
- [ ] Decision-making authority matrix (who can approve what during a crisis)
- [ ] 24/7 contact information for all crisis team members
- [ ] Secure crisis communication platform identified (not just email)

Regulatory Compliance

- [ ] Breach notification timeline documented for relevant regulations (SEC, FINRA, state laws)
- [ ] Required reporting forms and contact information for regulators readily accessible
- [ ] Legal counsel contact information (including after-hours emergency contact)
- [ ] Professional liability insurance policy reviewed for crisis response coverage
- [ ] Regulatory investigation response protocols documented

Communication Preparedness

- [ ] Client notification templates pre-approved by legal counsel
- [ ] Holding statements prepared for common crisis scenarios (breach, fraud, service failure)
- [ ] Stakeholder mapping completed (clients, partners, regulators, media, employees)
- [ ] Spokesperson identified and media trained
- [ ] Social media monitoring and response protocols established
- [ ] Website crisis banner and update protocols documented

Cybersecurity & Data Protection

- [ ] Data breach response plan integrated with overall crisis plan
- [ ] IT forensics firm identified and on retainer or pre-vetted
- [ ] Client data inventory maintained (what data exists, where it's stored)
- [ ] Cyber insurance policy reviewed for breach response coverage

- [ ] Credit monitoring service vendor identified for affected clients
- [ ] Encryption status documented for all sensitive client data

Scenario-Specific Protocols

- [ ] Response protocol for cybersecurity breach/ransomware
- [ ] Response protocol for employee misconduct (fraud, harassment)
- [ ] Response protocol for regulatory investigation or audit
- [ ] Response protocol for client dispute going public
- [ ] Response protocol for service failure causing client financial harm
- [ ] Response protocol for partnership dissolution or firm transition

Testing & Training

- [ ] Crisis plan tested through tabletop exercise in last 12 months
- [ ] All crisis team members trained on their roles and responsibilities
- [ ] Client-facing staff trained on what to say (and not say) during a crisis
- [ ] Crisis plan accessible to team members 24/7 (not just on office computers)
- [ ] After-action review process established to improve plan after incidents

SCORING YOUR READINESS

WHAT TO DO NEXT

If you checked fewer than 20 boxes: Schedule a Risk Assessment with Crisis IQ Partners to identify your most critical vulnerabilities and get a prioritized action plan.

If you checked 20-25 boxes: Your foundation is solid, but untested plans fail under pressure. Consider Crisis Response Training to ensure your team can execute when it matters.

If you checked 25+ boxes: You're ahead of most firms. Consider Advisory Support to maintain readiness as your firm evolves and new threats emerge.

Ready to close your gaps?

📞 Schedule a free 30-minute consultation: Select a Date & Time - Calendly
📧 Email us: Hello@crisisiqpartners.com
🔗 Take our 3-minute Crisis Readiness Scorecard: Crisis IQ Scorecard

Crisis IQ Partners, LLC | www.crisisiqpartners.com