RISK I.Q.
Internal Questionnaire

Robbery. Employee Fraud. Cyberattacks.

Unfortunate events like these can happen to any bank or credit union. Having a proactive plan for swift and thorough protection of your employees, data, and assets in the face of unexpected circumstances is paramount.

Answer the following questions to help you better understand potential risks related to your institution's data.

POLICY & COMPLIANCE OVERSIGHT

Focus: Audits, certifications, insurance, and regulatory alignment

Does your financial institution...

Perform annual, comprehensive, independent risk audits (e.g., SOC II) to identify internal/external threats?	☐ Yes	☐ No	☐ Unsure
Maintain high-level summaries of audits and corresponding remediation plans?	☐ Yes	☐ No	☐ Unsure
Require vendors to provide certifications/attestations (e.g., SOC II, ISO 27001)?	☐ Yes	☐ No	☐ Unsure
Meet insurance coverage requirements and confirm policy limits are adequate?	☐ Yes	☐ No	☐ Unsure
Collaborate with cross-functional teams and vendors on continuity plans that prioritize compliance?	☐ Yes	☐ No	☐ Unsure
Escalate confirmed security breaches within 36 hours in accordance with FDIC Computer-Security Incident Notification Final Rule?	☐ Yes	☐ No	☐ Unsure

RISK I.Q.
Internal Questionnaire

INTERNAL PROCESSES & SECURITY MEASURES

Focus: Physical and digital access controls, employee protocols, and fraud prevention behaviors

Does your financial institution...

Physical Threat Response

Maintain a specific response plan for physical threats (robbery, extortion, kidnapping, bomb threats)?	☐ Yes ☐ No ☐ Unsure
Practice use of bait money?	☐ Yes ☐ No ☐ Unsure
Routinely check authority limits for physical keys, fobs, and safe combinations?	☐ Yes ☐ No ☐ Unsure
Outline procedures for identifying and managing abandoned packages?	☐ Yes ☐ No ☐ Unsure
Maintain dual control over alarm systems?	☐ Yes ☐ No ☐ Unsure
Ensure minimal cash is held on teller lines?	☐ Yes ☐ No ☐ Unsure
Have a management/law enforcement notification plan?	☐ Yes ☐ No ☐ Unsure

Fraud Prevention & Data Controls

Require in-depth identifying information to authenticate new accountholders?	☐ Yes ☐ No ☐ Unsure
Require hard-to-guess passwords/passcodes for customer accounts?	☐ Yes ☐ No ☐ Unsure
Share cybersecurity best practices with accountholders?	☐ Yes ☐ No ☐ Unsure
Train staff on fraud warning signs and role-specific response procedures?	☐ Yes ☐ No ☐ Unsure
Split key functions/systems among staff to reduce data exposure?	☐ Yes ☐ No ☐ Unsure
Outline safe, compliant practices to prevent unauthorized or unlawful data use?	☐ Yes ☐ No ☐ Unsure
Limit data access to employees with a business need (e.g. principle of least privilege)?	☐ Yes ☐ No ☐ Unsure
Implement and maintain a fraud response plan?	☐ Yes ☐ No ☐ Unsure
Plan immediate communication protocols for discovered data threats?	☐ Yes ☐ No ☐ Unsure
Regularly review and revitalize data security procedures?	☐ Yes ☐ No ☐ Unsure

RISK I.Q.
Internal Questionnaire

TECHNOLOGY & ACCESS CONTROLS

Focus: Cybersecurity infrastructure, digital fraud defenses, and system-level safeguards

Does your financial institution...

Encrypt data and use antivirus and antispyware software?	☐ Yes	☐ No	☐ Unsure
House and monitor data 24/7/365 in physically secure environments?	☐ Yes	☐ No	☐ Unsure
Use MFA for employees, vendors, and accountholders?	☐ Yes	☐ No	☐ Unsure
Integrate biometrics (e.g., fingerprints, voice) into authentication layers?	☐ Yes	☐ No	☐ Unsure
Use complex passwords with strict expiration/reset protocols?	☐ Yes	☐ No	☐ Unsure
Identify all individuals and systems with data access privileges?	☐ Yes	☐ No	☐ Unsure
Apply zero-trust architecture principles—validate every user/device?	☐ Yes	☐ No	☐ Unsure
Maintain a list of all devices and locations where data is stored or processed	☐ Yes	☐ No	☐ Unsure
Frequently test safety systems: cameras, motion sensors, etc.?	☐ Yes	☐ No	☐ Unsure
Equip ATMs with security features and surround with lighting/barriers/cameras?	☐ Yes	☐ No	☐ Unsure
Escalate unauthorized access attempts against any part of your or a vendor's network?	☐ Yes	☐ No	☐ Unsure
Invest in fraud monitoring services for high-risk entry points (e.g., new accounts, contact changes)?	☐ Yes	☐ No	☐ Unsure
Use tools to catch counterfeit checks at the point of deposit?	☐ Yes	☐ No	☐ Unsure
Partner with vendors offering advanced fraud monitoring (e.g., dark web, SSN, address changes)?	☐ Yes	☐ No	☐ Unsure

RISK & RESILIENCE READINESS

Focus: Continuity planning, breach simulation, and vendor network risk management

Does your financial institution...

Simulate breach scenarios to test organizational readiness?	☐ Yes	☐ No	☐ Unsure
Simulate business continuity plans annually to confirm budget and planning sufficiency?	☐ Yes	☐ No	☐ Unsure
Establish plans for managing breaches involving vendors' vendors?	☐ Yes	☐ No	☐ Unsure
Collaborate with vendors to ensure robust continuity and recovery frameworks are in place?	☐ Yes	☐ No	☐ Unsure

Review your responses to identify areas of confidence and those needing further investigation.

For more risk education, sign up for Allied Insights at: alliedsolutions.net/subscribe

Allied Solutions®

alliedsolutions.net

2030-R4-3/26