ACA Aponix Cybersecurity Checklist

ACA Aponix®

Cyber-attacks continue to increase in frequency and sophistication, creating an imminent cyber security threat for all organizations. Data breaches in the first quarter of 2022 were **up 14% over a year ago**, according to the Identity Theft Resource Center (ITRC). Additionally, 92 percent of the data breaches in the first three months of 2022 resulted from **cyber-attacks**.

Regulators on a global scale are responding by launching new measures to combat the rise in cyber-attacks, including: the Security Exchange Commission's (SEC) proposed Cyber Security Risk Management Rule, the EU's Digital Operational Resilience Act (DORA), and China's Personal Information Protection Law (PIPL).

We recommend you review the following cybersecurity safeguards and evaluate your organization's threat readiness.

✓ Perform Annual Risk Assessments

A risk assessment helps companies understand and mitigate any existing risks to avoid negative impacts from common cybersecurity threats.

» Do you routinely validate and test your cyber security programs?

» Does your risk assessment cover multiple topic areas of concern (i.e., payment fraud, privacy, cyber threats)?

» Have you recently checked your organization's cloud environments (e.g.: Microsoft 365) for security updates?

✓ Conduct Network Testing and Vulnerability Assessments

Vulnerability assessments can help your company reduce the risk of the significant financial, operational, and reputational losses that can result from a breach from common cybersecurity threats.

» Do you conduct a network vulnerability assessment more than once a year?

» Have you tested the security of your internal/external network via penetration testing?

» When did you last complete **Cloud Security Testing**?

✓ Monitor Threat Intelligence

Cyber threats are constantly evolving, so it's important to stay on top of new threats and address them as quickly as possible.

» Do you monitor **cyber alerts** to remain up to date on the current risk landscape?

» Do you monitor newly registered domain names for potential impersonations of your organization with **DNS Monitoring**?

» Do you monitor your website domain to ensure no malicious duplicates exist?

For more information, contact us here.

✓ Maintain Written Policies, Procedures, and Governance

The SEC recommends that firms should consider conducting full **Business Continuity Planning (BCP) tests** *on an annual basis.*

» Have you completed a business impact analysis (BIA) before updating your business continuity plan (BCP)?
» Have you created/updated your incident response plan (IRP)?
» Do you have a written information security program (WISP) to safeguard your firm's information in accordance with privacy regulations and industry standards?

✓ Ensure Operational Resilience Before, During, and After Business Disruptions

The SECs **proposed cyber security rules for investment advisers and companies and European Commission's Digital Operational Resiliency Act (DORA)***, both highlight that operational resilience is a priority for regulators on a national and global scale.*

» Do you have buy in for enabling **operational resilience** across the enterprise?
» Do you understand the operational resilience regulatory requirements for your industry?
» Does your firm have policies and procedures to address foundational components of operational resilience— program governance, risk management, planning and testing, third-party risk management (TPRM), and reporting?

✓ Provide Staff Cybersecurity Training

Verizon's Data Breach Investigations Report from 2022 states that the most common cause of cyber breaches is human error. In 2022, 82% of breaches involved a human element.

» Is annual cybersecurity training required for employees of all levels?
» Have you sought out cost-effective resources such as online training courses in cybersecurity awareness?
» Do you conduct phishing campaigns within your company to test your employee's cybersecurity awareness?

✓ Conduct Scenario Testing and Mock Audits

Scenario testing and mock audits are two ways to determine your organization's ability to respond to and mitigate risk.

» If applicable, have you completed a regulatory mock exam in the past 6 months?
» Have you completed a tabletop exercise to test your response readiness?
» Have you researched ways to excel in testing instead of just meeting compliance requirements

For more information, contact us here.

✓ Refresh Your Vendor Due Diligence

Third-party risk management (TPRM) helps ensure your vendors protect your data, comply with regulations, and provide sustainable services that meet your requirements.

» Have you modified your assessment of vendor risk according to the product/service your vendor provides?

» When did you last review your vendor's current review practices, such as: maintaining SOC/SIG/AITEC documents, IRPs, certificates of insurance, etc.?

» Has your IT team created a risk-ranking system for vendors (ranking them as high, medium, or low risk) to critically evaluate vendor's adherence to due diligence requirements

✓ Review your Privacy Policies

Reviewing your privacy policies helps protect and mitigate risks within your firm's cybersecurity framework.

» Have you reviewed your privacy policies to ensure they meet the state, local, and federal guidelines? (e.g.: California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA) which amends the CCPA, and the EU & UK's General Data Protection Regulation (GDPR))

» Have you recently tested the design and effectiveness of your firm's privacy program implementation?

» Does your organization keep up to date with changes in the privacy landscape to adjust policies as needed?(e.g.: the Schrems II decision)

For more information, contact us here.