K3 TECHNOLOGY
IT, Security, and Cloud Solutions

DIY ASSESSMENT

CYBER INSURANCE READINESS CHECKLIST

Strengthen your defenses and ensure compliance with your cyber insurance policy.

Purpose and Objectives:

The Cyber Insurance Readiness Checklist is designed to support your organization in evaluating its readiness for obtaining a cyber insurance policy and staying compliant with policy requirements. This comprehensive tool delves into key aspects of cyber risk management specifically tailored to cyber insurance, although it should not be regarded as a formal risk assessment. The checklist helps you examine your existing information security controls, policies, employee training, and other factors that cyber insurance carriers often inquire about or mandate for your organization. Once completed, an analysis of this assessment will empower you to identify potential gaps and determine the necessary steps to ensure compliance with cyber insurance terms and conditions. This valuable resource is geared towards business owners and executives, providing a user-friendly and efficient way to navigate the world of cyber insurance and enhance your organization's overall security posture.

Key Sections:

- Network Security Controls
- Sensitive Data
- Compliance
- Privacy
- Payment Card Controls
- Business Continuity / Disaster Recovery / Incident Response
- Vendor Controls
- Outsourced Services
- MFA Attestation

Please note that this checklist is for informational purposes only and should not be considered as legal, financial, or insurance advice. It is always recommended to seek professional guidance tailored to your organization's unique circumstances.

GET IN TOUCH

303.770.8050 | www.k3techs.com | info@k3techs.com

NETWORK SECURITY CONTROLS

Indicate whether or not you have the following in place:

□ Chief Information Security Officer or other individual assigned responsibility for privacy and security practices

□ Up-to-date, active firewall technology

□ Up-to-date, active anti-virus software on all computers, networks, and mobile devices

□ A process in place to regularly download, test, and install patches. If Yes, is this process automated?
  □ If Yes, are critical patches installed within 30 days of release?

□ Intrusion Detection System (IDS)

□ Intrusion Prevention System (IPS

□ Data Loss Prevention System (DLP)

□ Multi-factor authentication for administrative or privileged access

□ Multi-factor authentication for remote access to the network, cloud and other systems and programs that contain private or sensitive data in bulk

□ Multi-factor authentication for remote access to email

□ Remote access to the organization's network limited to VPN

□ Backup and recovery procedures in place for all important business and customer data. If yes, are such procedures automated? IF yes, are such procedures tested on an annual basis?

□ Annual penetration testing. If Yes, is such testing conducted by a third party service provider?

□ Annual network security assessments. If yes, are such assessments conducted by a third party service provider?

□ Systematic storage and monitoring of network and security logs

□ Enforced password complexity requirements

□ Procedures in place to terminate user access rights as part of the employee exit process

SENSITIVE DATA

Complete the following:

□ Create and maintain a detailed list of all locations and applications where the following information type is stored: Credit/Debit card data, medical information/protected health information (PHI), bank account numbers, social security numbers, employee/HR information, intellectual property, personally identifiable information (PII)

□ Confirm that MFA is enabled to access any file shares or applications containing the above listed sensitive information

□ Confirm that encryption of data at rest is enabled for any file shares or applications containing the above listed sensitive information

□ Confirm that encryption of data in transit is enabled for any file shares or applications containing the above listed sensitive information

□ Confirm that encryption of data in-transit and at rest on mobile devices is enabled for any devices storing or accessing the above listed sensitive information (whether devices are owned by company, or owned by employees/users)

□ Confirm that data is encrypted while in the care, custody and control of a third-party service provider

COMPLIANCE

Complete the following:

- □ Is your business a Healthcare Provider, Business Associate, or Covered Entity under HIPAA? If Yes, are you HIPAA compliant?
- □ Is your business subject to General data Protection Regulation (GDPR)? If yes, are you currently compliant with GDPR?
- □ Is your business subject to the FTC Safeguards Rule (Auto Dealer, Mortgage broker, CPA firm, etc.)? If yes, are you currently compliant with the FTC Safeguards Rule?
- □ If your business is subject to any other regulations, list out what regulations, and visit the regulating body's website to determine if you are compliant with the requirements.

PRIVACY

Does your business handle any sensitive data listed in the sensitive data checklist on the previous page, which belongs to third-party end users? If so, answer the following:

- □ A Chief Privacy Officer or other individual assigned responsibility for monitoring changes instatutes and regulations related to handling and use of sensitive information
- □ A publicly available privacy policy which has been reviewed by an attorney
- □ Sensitive data classification and inventory procedures
- □ Data retention, destruction, and record keeping procedures
- □ Annual privacy and information security training for employees
- □ Restricted access to sensitive data and systems based on job function

PAYMENT CARD CONTROLS

Complete only if you, or a third party on your behalf, collects, processes, stores or accepts payment card information.

Indicate whether the current payment card environment:

- □ Processes all payment cards using End-to-End or Point-to-Point encryption
- □ Encrypts or tokenizes card data when stored
- □ Processes card present transactions using EMV capable devices

BUSINESS CONTINUITY / DISASTER RECOVERY / INCIDENT RESPONSE

Indicate whether you have the following in place:

- □ A disaster recovery plan, business continuity plan, or equivalent to respond to a computer system disruption.
- □ An incident response plan to respond to a network or system intrusion.
- □ Are all plans that are in place tested regularly with any critical deficiencies remediated? If so, how do you keep record of this?

Based upon testing results, how long does it take to restore your critical business operations following a network or system interruption? Think in terms of hours.

VENDOR CONTROLS

For vendors with access to your computer system or confidential information, indicate whether you have the following in place:

□ Written policies which specify appropriate vendor information security controls

□ Periodic review of, and updates to, vendor access rights

□ Prompt revocation of vendor access rights when access is no longer needed

□ Logging and monitoring of vendor access to your systems

□ A requirement that vendors carry their own Professional Liability or Cyber Liability insurance

□ Hold harmless / indemnity clauses that benefits you in contracts with vendors

OUTSOURCED SERVICES

Create and maintain a list of vendors your outsource services to, as they relate to your systems, networks, computers, and applications. Also maintain a central repository with the most recently signed contracts with these vendors. This should include vendors for: data backup, data center hosting, IT Infrastructure, IT security, web hosting, payment processing, physical security. software development, customer marketing and data processing.

MFA ATTESTATION

Indicate whether you have the following in place:

□ Is Multi-factor authentication (MFA) required for all employees and company users when accessing email through a website or cloud based service?

□ Is MFA required for all remote access to the networks provided to the employees and company users, contractors and 3rd party service providers?

□ In addition to remote access, is multi-factor authentication required for the following, including such access provided to 3rd party service providers:

□ All internal & remote admin access to directory services (active directory, LDAP, etc.).

□ All internal & remote admin access to network backup environments.

□ All internal & remote admin access to network infrastructure (firewalls, routers, switches, etc.).

□ All internal & remote admin access to the organization’s endpoints/servers.

Meet Requirements with K3

We understand that going through this checklist and ensuring all boxes are checked can be overwhelming. If you encounter any issues, have questions, or would like a professional assessment, please don't hesitate to reach out to us. Our team of experts is always here to help you make informed decisions and ensure you have the best protection in place.

Here's what we offer:

- A comprehensive Cyber Insurance Readiness Assessment
- Tailored solutions to address your specific needs
- Ongoing support and monitoring to maintain compliance with your cyber insurance requirements

With us in your corner, you'll be better prepared to qualify for cyber insurance, avoid losing coverage, and eliminate claim issues.

303.770.8050 | www.k3techs.com | info@k3techs.com