

# Cybersecurity Readiness Assessment

Preparing Your Business for the Unexpected



Designed to help organizations assess current cybersecurity controls and establish a road-map towards improved information security practices.

Organizations face cybersecurity risk on a daily basis and must fend off looming threats and protect against external intrusions. You can never be certain of your security stance unless periodic risk assessments are conducted. RCG's cybersecurity readiness assessment delivers actionable recommendations to improve your organization's information security posture and align with regulatory requirements and industry standards.

RCG's cybersecurity readiness review will evaluate internal controls to ensure they are comprehensive based on the National Institute of Standards & Technology (NIST) information security framework. RCG advisors can assist your business in meeting key stakeholder and audit expectations with specific guidance on remediation action and support to achieve compliance.

## Assessment Focus Areas:

**Cybersecurity Governance:** How does your organization delegate responsibility for cybersecurity? Are risk assessments periodically conducted to evaluate ever-changing cybersecurity risks? To what level is senior leadership and the board involved in cybersecurity preparedness?

**Network Security:** How does your organization monitor the network to identify and mitigate potential vulnerabilities? What measures are in place to detect, prevent, and correct network boundaries and hardware defenses to properly safeguard the environment?

**Access Rights & Controls:** What controls are in place to prevent unauthorized access to systems and data?

**Data Loss Prevention:** Is your organization properly safeguarding data with appropriate preventive controls?

**Vendor Management:** Has your organization conducted risk assessments for all third-party service providers?

**Incident Response & Business Continuity Planning:** How prepared is your organization to respond to and recover from a security incident or business disruption?

Are tabletop exercises conducted to review and become familiar with defined procedures?

**Training & Awareness:** How well do employees understand and follow organization protocols related to safeguarding privacy information and technology?

 [support@riskcompliancegroup.com](mailto:support@riskcompliancegroup.com)

Call us to discuss your situation and how we can provide support.

 330. 701. 1308