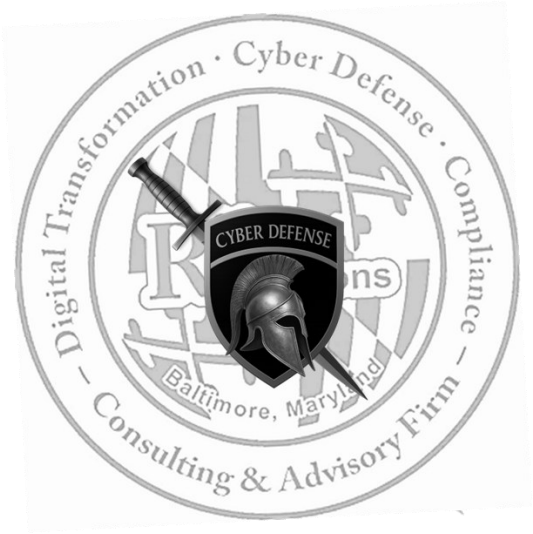
R32 Solutions



R32 Solutions
Executive Cyber Defense Intake Questionnaire (R32-ECI-001) — FY-2026 Edition

For Mission Critical Systems and Businesses

R32 Internal Doctrine – Website Use Only

R32 Solutions Executive Cyber Defense Intake Questionnaire

Introduction

The R32 Solutions Executive Cyber Defense Intake Questionnaire (R32-ECI-001) is designed to help regulated organizations evaluate their cybersecurity, compliance, and audit-readiness posture through a federal and executive lens.

Unlike traditional checklists or technical surveys, this questionnaire focuses on organizational defensibility—whether leadership, governance, and operational controls can withstand regulatory scrutiny, audit replay, legal examination, and executive accountability standards increasingly enforced across healthcare, government, financial services, energy, and other regulated sectors.

This questionnaire does not generate a score, rating, or certification outcome. Instead, it highlights where federal-grade expectations exceed current organizational readiness, signaling areas that commonly drive audit findings, enforcement actions, insurance pressure, and executive exposure.

Instructions

1. **Complete this questionnaire based on current operations — not future plans.**
   Regulators, auditors, insurers, and investigators evaluate the present state of operations.
2. **If uncertain about a response, indicate “In Progress” or “Unsure.”**
   Uncertainty itself represents a governance or readiness gap requiring leadership attention.
3. **This questionnaire should be completed by leadership or executive-level stakeholders.**
   Recommended participants include Executive Leadership, IT, Security, Compliance, Risk, Legal, and Operations.
4. **Protect this document.**
   It contains high-level operational insights that may reveal internal risk conditions. Treat it as a confidential internal record.
5. **Completion does not constitute engagement.**
   Organizations seeking an executive-level review may choose to share a completed copy with R32 Solutions through secure channels.

Section 1 — Organization Profile

(Complete all applicable fields. Use text or checkmarks as appropriate.)

- Organization Name: _____
- Industry / Sector: _____
- Number of Employees: _____

Primary Regulatory Exposure (check all that apply):
☐ Healthcare (HIPAA / CMS)
☐ Government / Defense
☐ Financial Services / Insurance
☐ Energy / Critical Infrastructure
☐ Other Regulated Environment: _____

- Executive Contact Name & Title: _____
- Business Email: _____
- Phone (optional): _____

Section 2 — Executive Risk Signals

(Check all statements that apply to your organization today.)

☐ We operate under formal regulatory, contractual, or audit requirements
☐ A failed audit, investigation, or breach would materially impact operations, revenue, or reputation
☐ Cyber insurance requirements or premiums have increased in the last 12 months
☐ Executive leadership is directly accountable for cybersecurity or compliance outcomes
☐ We rely on third parties, MSPs, or vendors for critical systems or sensitive data
☐ We have experienced a security incident, investigation, audit concern, or near-miss

Section 3 — Governance & Readiness Overview

(Indicate the most accurate response for each item.)
Response options: Yes | In Progress | No

- Formal cybersecurity governance structure: ☐ Yes ☐ In Progress ☐ No
- Documented policies and operational controls: ☐ Yes ☐ In Progress ☐ No
- Incident response and breach escalation capability: ☐ Yes ☐ In Progress ☐ No
- Audit evidence and documentation readiness: ☐ Yes ☐ In Progress ☐ No
- Executive or board-level oversight of cyber risk: ☐ Yes ☐ In Progress ☐ No

(No frameworks, standards, or methodologies are disclosed at this stage.)

Section 4 — Engagement Intent

(Optional but recommended.)

- What prompted you to reach out to R32 Solutions?

Anticipated timeframe for action:
☐ Immediate (0–30 days)
☐ Near-term (30–90 days)
☐ Planning (90+ days)

Primary area of interest:
☐ Executive Advisory / Strategic Support
☐ Audit Readiness & Defensibility
☐ Cyber Defense Strategy
☐ Exploratory / Not Sure

Section 5 — Confidentiality & Intellectual Property Notice

Confidentiality & Intellectual Property Notice

This questionnaire, including its structure and content, constitutes proprietary intellectual property of R32 Solutions, LLC. It is provided solely for the purpose of evaluating a potential professional engagement.

No portion of this material may be copied, reproduced, reverse-engineered, distributed, or used for competitive or commercial purposes without the express written consent of R32 Solutions.

Completion or submission of this document does not create a client relationship.

Closing Statement

This questionnaire is intended to provide a high-level executive perspective on cybersecurity, compliance, and audit readiness. It does not constitute legal advice, a formal audit, or a certification review.

Treat this document as confidential internal material. Access should be limited to senior leadership and appropriate governance officials.

Do not include Protected Health Information (PHI) or Personally Identifiable Information (PII).
Responses should describe processes, structures, and organizational readiness only.

Organizations requesting an executive-level review should submit a sanitized copy through secure channels.

Data Handling Notice

Do not include PHI or PII in this document. All shared materials must be sanitized and will be treated as confidential under R32 Solutions' proprietary intake and advisory doctrine.

Point of Contact — R32 Solutions

(Submit sanitized documents only.)

Remi Silva
Owner & CEO
R32 Solutions
Email: remi@r32solutions.com
Phone: (410) 570-9715

Fanta Whiting
Partner
R32 Solutions
Email: fanta@r32solutions.com
Phone: (202) 672-3760