RCA-50™ Cyber Readiness Framework

Overview

A structured approach to evaluating cybersecurity maturity, risk exposure, and readiness

Designed for small and mid-sized businesses, healthcare organizations, and regulated environments.

© PS Cyber Defense Institute™
Confidential Overview

---

1. Introduction

Cybersecurity risk is no longer limited to large enterprises. Small and mid-sized organizations face increasing exposure to ransomware, phishing, regulatory scrutiny, and third-party risk—often without the internal resources to clearly assess their current standing.

The **RCA-50™ Cyber Readiness Framework** was created to provide organizations with a clear, structured, and practical way to understand their cybersecurity posture, identify priority risks, and guide improvement decisions.

Rather than focusing solely on technical controls or compliance checklists, RCA-50™ evaluates **real-world readiness**—how effectively people, processes, and technology work together to manage cyber risk.

---

2. What Is the RCA-50™ Framework?

The RCA-50™ Cyber Readiness Framework is a **50-control assessment model** designed to measure cybersecurity maturity across critical operational and governance areas.

It is intended for leadership teams who need:

- A realistic view of current cyber readiness
- Clear identification of key risk areas
- Actionable guidance—not raw technical data

RCA-50™ aligns conceptually with widely recognized security standards such as NIST and HIPAA, while remaining accessible to non-technical stakeholders.

The framework emphasizes **clarity, prioritization, and practicality** over exhaustive technical depth.

---

3. What the RCA-50™ Evaluates

RCA-50™ evaluates cybersecurity readiness across **five core domains**, together providing a comprehensive view of organizational risk.

1. People & Cyber Awareness

Evaluates workforce readiness, including security training, phishing awareness, reporting culture, and staff behavior.

2. Technology & Infrastructure

Assesses technical safeguards, including email security, patching practices, backups, endpoint protection, and device security.

3. Policies & Governance

Reviews the existence and maturity of security policies, documentation, incident response planning, and governance alignment.

4. Identity & Access Controls

Examines how user access is managed, including passwords, multi-factor authentication (MFA), privileged access, and account reviews.

5. Operations & Incident Response

Evaluates monitoring, logging, vendor oversight, and preparedness to detect, respond to, and recover from cyber incidents.

Together, these domains help identify not only where gaps exist, but **which gaps matter most**.

---

4. RCA-50™ Cyber Maturity Model

RCA-50™ uses a **five-tier maturity scale** to reflect how consistently cybersecurity controls are implemented and managed.

Maturity Level	Description
Level 1 — Foundational	Controls are limited, informal, or largely reactive.
Level 2 — Developing	Some controls exist but are inconsistently applied or documented.
Level 3 — Defined	Controls are documented, implemented, and repeatable.
Level 4 — Managed	Controls are mature, monitored, and regularly reviewed.
Level 5 — Optimized	Cybersecurity is integrated, measured, and continuously improved.

This model is designed to **guide improvement**, rather than assigning blame or certifying compliance.

5. Assessment Options

The RCA-50™ Framework can be used in two ways, depending on the level of guidance required.

RCA-50™ Snapshot (Free)

The Snapshot is a self-guided assessment that provides immediate, high-level insight.

Includes:

- 50-question self-assessment
- Automated scoring
- Overall maturity tier
- High-level summary

Best for:
Organizations seeking quick awareness and a baseline understanding of cyber readiness.

Guided RCA-50™ Assessment (Flagship Offering)

The Guided assessment adds expert interpretation and strategic guidance.

Includes:

- Expert review and validation of responses
- Executive-ready cyber risk report
- Domain-level findings with business impact
- Prioritized recommendations
- 30-60-90 day action roadmap

Best for:
Leadership teams need clarity, defensible documentation, and a practical improvement plan.

---

6. Privacy & Confidentiality

All RCA-50™ assessment responses are treated as confidential and are used solely for the purpose of delivering assessment results.

Assessment data is **not shared, sold, or reused**.

RCA-50™ is a cyber readiness and risk-identification framework. It is **not**:

- A compliance certification
- A penetration test
- A guarantee of security

---

7. Using RCA-50™ Results

Organizations commonly use RCA-50™ results to:

- Support leadership and board discussions
- Prioritize cybersecurity investments
- Inform remediation planning
- Prepare for audits, insurance reviews, or regulatory inquiries

The framework is designed to support **informed decision-making**, not fear-based urgency.

8. Next Steps

Organizations may:

- Begin with the **free RCA-50™ Snapshot** to establish a baseline
- Upgrade to the **Guided RCA-50™ Assessment** for expert insight and planning
- Use results as a foundation for ongoing cybersecurity improvement

Learn more at:
www.psdefense.academy

© PS Cyber Defense Institute™
All rights reserved.