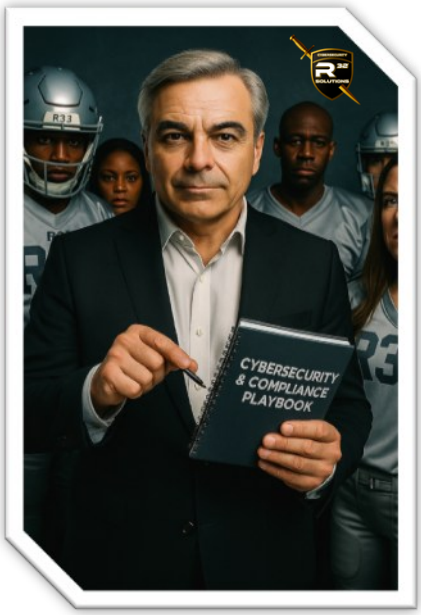
Cyber Defense. Audit-Ready.

R32 Solutions Playbook

Strategic Objective

This playbook serves as a high-level strategic guide for cybersecurity and compliance leadership across mission-critical sectors. It is designed to deliver concierge-level cybersecurity strategy and enterprise-grade compliance, enabling organizations to secure infrastructure, exceed regulatory expectations, and maintain continuous audit readiness.

R32 Solutions aligns internal leadership, IT teams, MSPs, and vendors with leading frameworks—including NIST, SOC 2, ISO 27001, and other federal and industry mandates—to ensure operational resilience, audit success, and zero disruption in high-risk environments.



Developed by: R32 Solutions (R32) 2025

PLAY 1

Discovery & Risk Landscape Mapping

Objective: Understand the full scope of your organization's digital, operational, and risk environment.

Key Actions:

- Inventory infrastructure, assets, users, vendors, and critical systems.
- Map business processes to security and compliance obligations.
- Identify existing frameworks in use (NIST, ISO, SOC 2, etc.).
- Capture known vulnerabilities, past incidents, and insurance requirements.

Outcome: A current-state operational and risk profile that frames all subsequent planning.

PLAY 2

Engagement Strategy & Governance Design

Objective: Define a leadership-aligned strategy and governance model to guide cybersecurity and compliance transformation.

Key Actions:

- Identify internal stakeholders, IT, MSPs, and vendors for collaboration.
- Establish vCISO/vCIO advisory and governance meeting cadence.
- Define strategic goals tied to regulatory mandates and risk appetite.
- Align roles and responsibilities to HIPAA, NIST, ISO, SOC 2, and GDPR.

Outcome: A unified governance and strategy foundation for compliance-led execution.

PLAY 3

Gap Analysis & Control Assessment

Objective: Identify regulatory gaps, cybersecurity control weaknesses, and audit readiness deficiencies.

Key Actions:

- Conduct a NIST 800-53 and ISO 27001-based control assessment.
- Evaluate existing policies, procedures, technical safeguards, and training.
- Perform HIPAA Security Risk Assessment (SRA) and vendor risk reviews.
- Map deficiencies to high-risk operational exposures.

Outcome: A prioritized roadmap for remediation and improved security posture.

PLAY 4

Penetration Testing & Technical Validation

Objective: Test the resilience of your infrastructure, systems, and staff against real-world threats.

Key Actions:

- Conduct internal and external penetration tests (aligned to OWASP, PTES).
- Simulate phishing, ransomware, and privilege escalation attacks.
- Identify exploitable vulnerabilities and validate security controls.
- Deliver detailed findings report with risk scoring and impact mapping.

Outcome: Real-world visibility into exploitable weaknesses before attackers find them.

PLAY 5

Remediation, Policy Hardening & Documentation

Objective: Strengthen systems, correct control weaknesses, and align documentation with federal requirements.

Key Actions:

- Implement technical fixes, configuration baselines, and MFA enforcement.
- Update policies to align with NIST, HIPAA, CMMC, SOC 2, and ISO 27001.
- Create training plans, vendor protocols, and data governance SOPs.
- Prepare attestation materials and build an Audit-Ready Binder.

Outcome: A secure, documented, and policy-aligned environment ready for regulatory review.

PLAY 6

Sustainment & Continuous Improvement

Objective: Maintain audit-readiness, operational resilience, and compliance maturity over time.

Key Actions:

- Launch quarterly tabletop exercises and mock audits.
- Monitor security operations with automated alerting and logging.
- Update risk register, training logs, and incident reports routinely.
- Conduct quarterly governance reviews with IT, leadership, and R32 advisors.
- Maintain active compliance with MSP, vendors, and new tech integrations.

Outcome: Long-term compliance resilience and enterprise-level cybersecurity maturity.

R32 Solutions® – Concierge-Level Security. Audit-Ready. Resilience Delivered.