Cyber Defense. Audit-Ready.

# R32 Cybersecurity & Compliance Packages

Built for Government, Defense, Healthcare, and Critical Industries — Scalable for All

## Introduction & Purpose

R32 Solutions is a trusted cybersecurity and compliance integrator specializing in the defense of mission-critical systems across government, defense, healthcare, technology, and regulated commercial sectors. We help organizations strengthen their security posture, align with leading regulatory frameworks, and maintain continuous audit and certification readiness in high-stakes environments.

Our mission is to equip executive leadership and IT stakeholders with actionable intelligence, standards-aligned assessments, and expert-led remediation services that protect infrastructure, reduce risk, and ensure operational continuity.

To support this mission, R32 Solutions offers a suite of structured Cybersecurity & Compliance Packages—each designed to meet organizations at critical points in their security lifecycle. Whether you are conducting a first-time assessment, remediating known issues, or requiring embedded leadership to guide complex regulatory programs, our offerings deliver scalable, defensible results grounded in NIST SP 800-53, NIST SP 800-171, HIPAA Security Rule, and ISO/IEC 27001:2022.

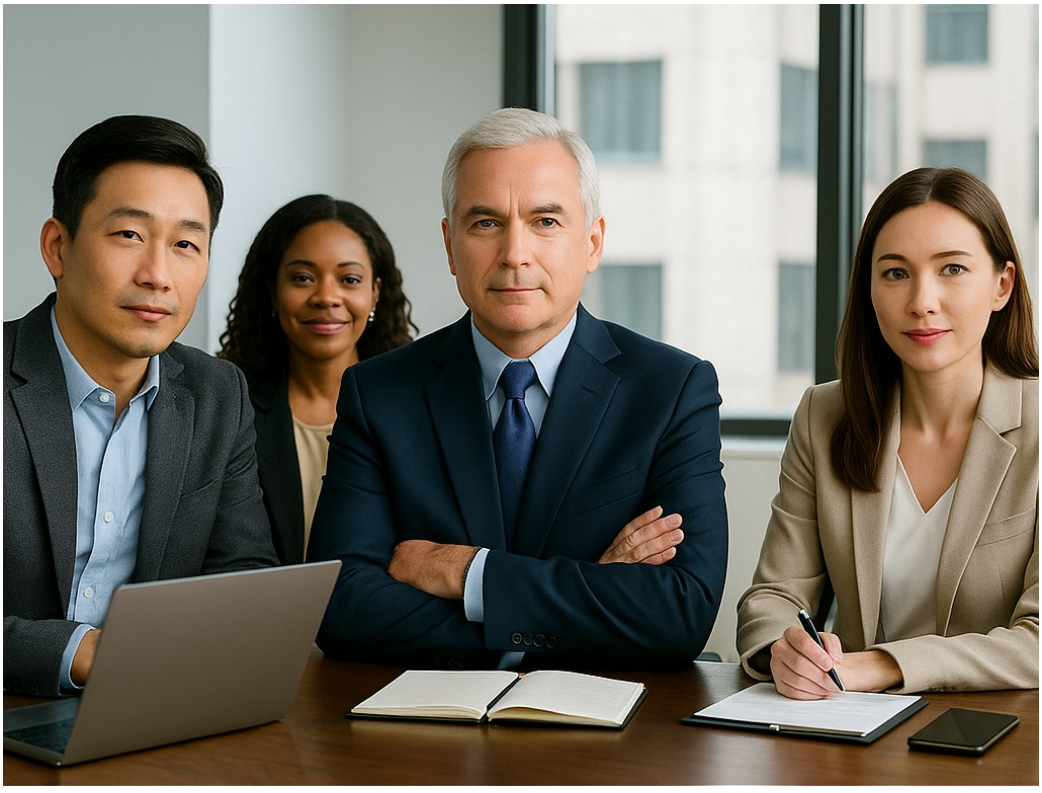
- **The Baseline Package** delivers a comprehensive cybersecurity health check and compliance posture snapshot.
- **The Remediation & Readiness Package** combines technical and policy remediation with certification-grade preparation and audit readiness.
- **The Concierge Oversight Package** provides embedded executive leadership for long-term cybersecurity governance, audit strategy, and real-time advisory support.

All packages are designed for scalability, documentation rigor, and technical alignment with both U.S. federal and international cybersecurity frameworks.

In addition, R32 Solutions offers executive-level consulting and virtual CISO (vCISO) services to support boards, managed service providers (MSPs), compliance teams, and legal counsel in navigating live audits, breach response, and enterprise transformation projects requiring governance-level leadership and evidence-grade documentation.

This document outlines each package in detail to help you make informed decisions that protect your systems, secure your operations, and strengthen your mission.

R32 Cybersecurity and Compliance Assessment Team



# Baseline Package: Cybersecurity Health Check

## Purpose

This package delivers a foundational cybersecurity and compliance assessment aligned with NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, HIPAA Security Rule, and ISO/IEC 27001:2022. It is designed to help organizations identify vulnerabilities, evaluate control gaps, and establish a roadmap for regulatory compliance, audit readiness, and infrastructure hardening.

---

## Engagement Scope & Workflow

### 1. Kickoff & Discovery

- Project kickoff with stakeholders and designated R32 Cyber Strategist
- Environment scoping: network topology, enclaves, cloud/on-prem footprint
- Information request and documentation intake (policies, diagrams, inventories)
- Access coordination for scan setup and interviews

### 2. Interviews & Technical Collection

- Stakeholder interviews (IT, compliance, security, HR, operations)
- Targeted technical sessions to assess access control, endpoint, and network defense
- End-user awareness and hygiene posture review

### 3. Risk & Compliance Assessment

- Internal and external vulnerability scans (non-intrusive)
- Baseline Security Risk Assessment (aligned with HIPAA and ISO/IEC 27001)
- Control mapping against NIST SP 800-53 or NIST SP 800-171 (client-selected)
- Review of administrative, technical, and physical safeguards
- Targeted policy gap review of access, incident response, and encryption standards

### 4. Strategic Checkpoints

- Mid-engagement findings review with preliminary observations
- Draft risk register review and prioritization
- Remediation roadmap alignment session

### 5. Final Reporting & Outbrief

- Executive outbrief presentation with summary of key risks and recommendations
- Comprehensive findings report detailing vulnerabilities, compliance gaps, and framework alignment
- Compliance scorecard and maturity heatmap
- 30-60-90 day remediation roadmap tailored to your organization's operational context
- Strategic guidance document to support executive decision-making and next-step planning

---

## Estimated Level of Effort

Estimated at 32 to 40 hours, depending on the number of systems, network complexity, regulatory scope, number of enclaves, and stakeholder availability. Additional effort may be required for larger or segmented environments.

---

## Assessment Duration

Typically completed within two weeks, subject to timely access to documentation, systems, and staff. Timelines may adjust depending on client responsiveness, infrastructure scale, and concurrent assessments.

---

## Framework References

- NIST SP 800-53 Rev. 5
- NIST SP 800-171 Rev. 2
- ISO/IEC 27001:2022
- HIPAA Security Rule (45 CFR §164 Subpart C)

---

## Pricing

Final pricing will be determined following an introductory scoping session. Pricing depends on network scale, system diversity, enclave segmentation, regulatory scope, and overall organizational complexity. All estimates are finalized upon mutual agreement and formal proposal issuance.

# Remediation & Readiness Package: Compliance Hardening & Certification Preparation

## Purpose

The Remediation & Readiness Package builds directly on findings from the Baseline Cybersecurity Health Check. It is designed to close identified gaps, implement controls, and develop defensible documentation that meets the expectations of regulators, cyber insurers, and certification bodies.

This package is ideal for organizations preparing for formal certification, addressing audit findings, or strengthening their cybersecurity program in collaboration with internal IT teams, managed service providers (MSPs), and third-party vendors. All work is aligned to NIST SP 800-53, NIST SP 800-171, HIPAA Security Rule, and ISO/IEC 27001:2022.

## Ideal For

- Organizations completing Phase 2 after the Baseline Package
- Environments with known gaps requiring remediation
- Pre-certification or pre-audit initiatives
- IT teams, MSPs, or vendors seeking support on compliance execution
- Organizations under regulatory scrutiny or preparing for enterprise growth

## Package Scope

| Phase | Activities & Deliverables |
|---|---|
| Kickoff & Scoping | Joint session with leadership, IT, MSPs, vendors to define workstreams |
| Gap Remediation Planning | Develop tactical remediation plans mapped to Baseline findings |
| Policy & Documentation Buildout | Draft, revise, or implement missing policies and procedures |
| Technical Control Implementation | Partner with IT/MSPs to implement endpoint, network, and access controls |
| Compliance Alignment Workshops | Focused sessions for HIPAA, NIST, ISO/IEC framework compliance |
| Staff Training & Awareness | Provide education materials and optional live sessions |
| Security Roadmap Finalization | Deliver maturity roadmap for next 6–12 months |
| Readiness Review & Outbrief | Executive-level reporting on progress, outstanding items, and audit readiness status |

## Engagement Details

- Duration: 4–6 weeks (varies by environment complexity)
- Stakeholders: Internal IT teams, MSPs, vendors, compliance managers, executives
- Frameworks Supported: NIST SP 800-53/800-171, HIPAA Security Rule, ISO/IEC 27001:2022
- Delivery Format: Remote and/or on-site support (as needed)

---

## Pricing

Pricing is customized based on scope, technical depth, and stakeholder complexity. Final pricing provided after Baseline Package completion or a formal discovery session.

# Concierge Oversight Package: Executive vCIO/vCISO Leadership & Governance

## Purpose

The Concierge Oversight Package provides fully embedded vCIO/vCISO leadership, delivering enterprise-grade cybersecurity, compliance, and IT governance across your organization. Tailored for high-risk and highly regulated environments, this engagement offers direct executive-level support for boards, compliance committees, MSPs, vendors, and internal IT leadership—ensuring strategic alignment, audit resilience, and operational continuity.

This is R32's most comprehensive and high-value offering—built for organizations that cannot afford security failure, compliance delays, or misalignment between technology and business objectives.

## Ideal For

- Organizations managing complex IT environments or multi-site operations
- Clients requiring senior leadership without hiring a full-time CIO or CISO
- Entities preparing for or responding to audits, certifications, or regulatory scrutiny
- MSP-led or hybrid environments seeking program continuity and strategic oversight
- Boards and C-suite executives who need trusted cyber risk translation and decision support

## Package Scope

| Domain | Oversight Activities & Deliverables |
|---|---|
| Executive Cyber Strategy | Full vCIO/vCISO support: roadmap design, resource alignment, security program leadership |
| Audit & Certification Governance | Direct coordination during live audits (HIPAA, SOC 2, ISO, CMMC), regulator inquiries, or pre-certification phases |
| Board & Leadership Reporting | Monthly or quarterly briefings with risk summaries, compliance KPIs, and executive insights |
| IT & Cyber Policy Management | Oversight of documentation lifecycle including Access Control, IR, Encryption, BCDR, and vendor security agreements |
| Risk Management & Metrics | Real-time risk register ownership, threat modeling, and remediation dashboards with NIST/ISO tracking |
| MSP & Vendor Alignment | Continuous collaboration with MSPs, cloud vendors, and third parties to ensure consistent compliance execution |

| | |
|---|---|
| Incident Response & Escalation | On-call executive advisory during breach events, regulatory disclosures, and legal coordination |
| Strategic IT Roadmap & Program Reviews | Alignment of business goals with IT and security strategy, maturity planning, and program optimization |

## Engagement Details

- **Duration:** 6 to 12 months recommended
- **Cadence:** Weekly, biweekly, or monthly strategic sessions
- **Delivery Format:** Remote-first with optional on-site leadership days
- **Stakeholders:** CIOs, CISOs, MSPs, vendors, legal counsel, executives
- **Frameworks Supported:** NIST SP 800-53, NIST SP 800-171, HIPAA Security Rule, ISO/IEC 27001, SOC 2 Type II, CMMC

## Pricing

Due to the scope and strategic impact of this offering, pricing is based on your organization's complexity, certification goals, and level of executive integration required. Final estimates are provided after a discovery and scoping session.

## Positioning Statement

With this package, R32 Solutions serves as a trusted extension of your leadership team—supporting your internal experts, enhancing decision-making, and providing steady guidance through complex cybersecurity, IT, and compliance challenges. Our goal is to empower your organization with clarity, confidence, and continuity—without disruption or overreach.

## Notes, Disclaimers, and Assumptions:

• Pricing Disclosure: Final pricing will be provided following a collaborative discussion and a comprehensive review of your organization's size, operational scope, compliance maturity, and the level of effort required to meet regulatory objectives. All pricing is subject to change based on actual conditions and client-specific requirements.

• Scope & Customization: This service package is intended as a flexible framework. Customizations may be necessary based on the nature of your organization technology infrastructure, staffing model, and current compliance posture.

• Add-On Services: Optional enhancements—such as cloud security reviews, third-party risk assessments, penetration testing, or red team engagements—can be integrated into any package tier for an additional fee.

• Assumptions: This proposal assumes reasonable access to internal stakeholders, IT systems, policies, and documentation needed to perform assessments and deliver solutions in a timely and secure manner. Delays or limitations in access may affect the timeline and scope of deliverables.

• Engagement Requirements: Formal engagement will require a signed service agreement, mutual confidentiality terms, and an agreed-upon scope of work (SOW) prior to initiation of services.