

Checklist: 5 Signs Your Healthcare Compliance Program Is Outdated

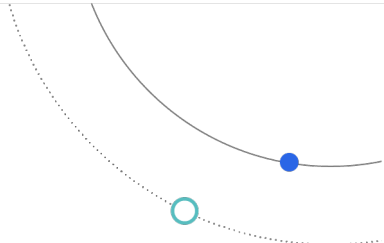
From C1 | For Healthcare CISOs, Compliance Officers, Risk Managers, and IT Security Leaders

Compliance Isn't Just a Checkbox Anymore

In today's healthcare landscape, regulatory compliance and cybersecurity are no longer separate conversations. The rising complexity of regulations—HIPAA, HITECH, 42 CFR Part 2, and evolving state privacy laws—collides with a surge in ransomware, insider threats, and phishing attacks targeting patient data.

If your compliance program still relies on spreadsheets, periodic risk reviews, or disconnected systems, you may be operating with blind spots that put your patients, data, and clinical operations at risk.

This checklist will help you evaluate your program's resilience and maturity, and show how C1's Advisory, Professional, and Managed Services can help transform compliance from a manual, reactive obligation into a continuous, technology-enabled advantage.



Checklist: 5 Signs Your Healthcare Compliance Program Is Outdated

1 Do you currently have a designated CISO or cybersecurity leader?

Yes No Not Sure

Why This Matter:

A clearly defined cybersecurity leader provides strategic direction, drives accountability, and ensures executive visibility. Without this role, security programs often become fragmented, underfunded, and reactive.

Industry Insight:

Organizations with a CISO detect and contain threats **30% faster** and save an average of **\$1.23 million per breach** (IBM Cost of a Data Breach Report).

C1 Solution:

- C1 vCISO Services offer a dedicated virtual CISO to lead and mature your cybersecurity program.
- We ensure alignment between cybersecurity and business priorities through executive engagement.
- C1 delivers structured reporting, board-level updates, and measurable KPIs to guide decision-making.

2 Have you performed a formal cybersecurity risk assessment in the last 12 months?

Yes No Not Sure

Why This Matter:

Risk assessments identify vulnerabilities, prioritize investments, and support informed decision-making. Without them, organizations lack visibility into their true threat landscape.

Industry Insight:

Organizations that conduct annual assessments aligned to frameworks like NIST or ISO are **40% less likely** to suffer severe cybersecurity incidents (Gartner).

C1 Solution:

- C1 conducts structured assessments using NIST CSF, ISO 27001, NIST 800-53, and more.
- We identify control gaps and create a Plan of Action and Milestones (POAM) to guide remediation.
- Our quarterly updates reflect evolving risks, compliance requirements, and operational changes.

3 Are you confident that your organization is fully compliant with applicable regulations (e.g., HIPAA, CMMC, NIST 800-171)?

Yes No Not Sure

Why This Matter:

Non-compliance can result in fines, failed audits, reputational damage, and missed business opportunities, especially in regulated industries.

Industry Insight:

HIPAA violations can reach **\$1.5 million annually**, and **30%** of audited breaches are linked to compliance failures (HHS OCR, CISA).

C1 Solution:

- C1 maps your security controls to compliance requirements such as HIPAA, PCI, and CMMC.
- Our vCISO provides ongoing monitoring and remediation oversight.
- We support policy development, control testing, and audit preparation to ensure compliance readiness.

4 Are sensitive data types (e.g., PII, PHI, cardholder data) properly classified and protected?

Yes No Not Sure

Why This Matter:

Poor data classification puts sensitive information at risk and hampers access control, encryption, and incident response.

Industry Insight:

Organizations that properly classify and encrypt data save an average of **\$360,000 per breach** (IBM Security). Implementing DLP tools reduces insider threat risks by **over 50%**.

C1 Solution:

- C1 Advisory assesses access control gaps and identity governance
- Professional Services implement logging, access control, and anomaly detection
- Managed Services monitor PHI access activity and generate compliance-aligned alerts

5 Do you evaluate the cybersecurity posture of third-party vendors before onboarding?

Yes No Not Sure

Why This Matter:

Vendors often access critical systems or sensitive data. Without robust third-party risk management, supply chain breaches become your liability.

Industry Insight:

60% of breaches stem from third-party vulnerabilities (Ponemon Institute). Regulators and insurers now require documented vendor risk assessments.

C1 Solution:

- C1 integrates third-party risk management into your broader security assessments.
- We offer templates, scoring models, and onboarding workflows to streamline vendor oversight.
- Our vCISO aligns your vendor program with NIST, ISO 27001, and CMMC standards.

How Did You Score?

# of "Yes" Answers	What It Means
5 of 5	Strong foundation—C1 can help you automate and scale.
3-4	Good progress—C1 can close remaining gaps.
0-2	High risk – C1 can modernize your program before the next audit or incident.



Why Healthcare Leaders Choose C1 for Compliance & Risk Management

C1 helps healthcare organizations shift from outdated, manual models to modern, continuous compliance and cyber resilience.



C1 Advisory Services

Strategic planning to align risk, security, and compliance across your organization:

- Regulatory framework alignment (HIPAA, NIST, HITRUST, 42 CFR)
- Executive workshops and board-level reporting strategies
- Zero Trust and risk mitigation roadmaps
- Business continuity and incident response strategy



C1 Professional Services

Turnkey deployment and configuration of risk-aware compliance solutions:

- Integration of SIEM, IAM, DLP, and compliance automation tools
- PHI monitoring infrastructure and alert logic customization
- Control mapping and audit trail generation
- Role-based access and identity policy configuration

Bottom Line:

Compliance today must be continuous, context-aware, and fully integrated with cybersecurity. C1 delivers the strategy, tools, and services that modern healthcare organizations need to stay secure, compliant, and prepared.

Talk with a C1 Expert

Let's go through your checklist together—and show you how to evolve your compliance program for stronger security, better audit outcomes, and less operational strain.



C1, the global technology solutions provider, transforms businesses by creating connected experiences that shape the future. With more than 6,000 customers, C1 empowers industries through secure, innovative technologies, collaborating with leading partners to deliver total lifecycle solutions. Learn more at onec1.com.