The Compliance Readiness Checklist

CMMC • SOC 2 • HIPAA Security • ISO 27001

Most companies don't fail audits because of sophisticated attacks. They fail because nobody stopped long enough to answer basic questions: Where does our sensitive data live? Who has access? What would an assessor ask first? This checklist is those questions, the same ones we walk through with every new BlueSteel client. Check what you have. What's left unchecked is your roadmap.

How to use it: Start with the Universal Core, it applies no matter which framework you're pursuing. Then jump to your framework section. Score yourself at the end.

The Universal Core (every framework starts here)

If you can't check at least 7 of these, fix this list before spending money on any audit.

☐	A named security owner (even fractional/vCISO) with executive backing and budget authority
☐	Complete asset inventory: every system, device, and cloud service that touches sensitive data
☐	A data map: where sensitive data lives, how it flows, and who actually has access today
☐	MFA enforced everywhere, least-privilege access, and documented onboarding/offboarding
☐	Core written policies (infosec, acceptable use, incident response, vendor management) reviewed in the last 12 months
☐	A risk assessment completed in the last 12 months, with a remediation plan that has owners and dates
☐	Security awareness training for all staff, at least annually, with completion records
☐	Centralized logging and monitoring on critical systems (you can answer: would we know if something happened?)
☐	Tested backups and a documented disaster recovery procedure that is tested, not just written
☐	An incident response plan that has been tabletop-exercised in the last 12 months

CMMC: Defense Contractors

DoD contracts are already requiring this. Miss the deadline, lose the revenue.

- [ ] You know which CMMC level your contracts require (Level 1 self-assessment vs. Level 2 certification)
- [ ] You've identified where CUI and FCI actually live, and scoped (shrunk) the assessment boundary
- [ ] NIST 800-171 self-assessment completed and your SPRS score is submitted and current
- [ ] System Security Plan (SSP) written, current, and reflects reality, not aspiration
- [ ] POA&M; in place for every gap, with named owners and realistic dates
- [ ] FIPS-validated encryption protecting CUI at rest and in transit
- [ ] Flow-down requirements addressed with every subcontractor touching CUI
- [ ] C3PAO assessment timeline mapped against your contract award deadlines (assessor calendars fill up fast)

SOC 2: SaaS & Services Companies

Usually triggered by a deal in your pipeline. The audit window means the clock is real.

- [ ] Trust Services Criteria selected: Security is mandatory, you've deliberately chosen (or excluded) the rest
- [ ] Report type decided: Type I (point in time) vs. Type II (observation window), and your sales team knows the timeline
- [ ] Every control mapped to a criterion and documented, no orphan controls, no unmapped criteria
- [ ] Evidence collection systematized (compliance platform or disciplined process), not a quarterly panic
- [ ] Subservice organizations reviewed: you've read your critical vendors' SOC 2 reports
- [ ] Change management and SDLC controls documented and actually followed by engineering
- [ ] A readiness/gap assessment done through an auditor's lens before the real audit
- [ ] Auditor selected, engagement letter signed, and the window aligned to your sales commitments

HIPAA Security Rule: Healthcare & Their Vendors

Applies to covered entities AND business associates. 'We're just the software vendor' is not an exemption.

- [ ] A designated HIPAA Security Officer, named in writing, not implied
- [ ] Security Risk Analysis completed and documented (its absence is OCR's most-cited finding)
- [ ] Full ePHI inventory: every system, device, and application that creates, stores, or transmits ePHI
- [ ] Business Associate Agreements signed with every vendor that touches ePHI, including AI tools
- [ ] ePHI encrypted at rest and in transit, or documented, defensible reasons why not
- [ ] Workforce HIPAA training completed and documented (proof matters as much as training)
- [ ] Contingency plan in place: data backup plan, disaster recovery plan, emergency mode operations
- [ ] Breach notification procedures documented, and your team knows the clock starts at discovery

ISO 27001: Selling Globally or to Enterprises

The international gold standard. Heavier lift, but one certification answers many questionnaires.

- [ ] ISMS scope defined and documented, which parts of the business are in, which are out, and why
- [ ] Risk assessment methodology defined, applied, and producing a risk treatment plan
- [ ] Statement of Applicability (SoA) drafted against all Annex A controls, with justified exclusions
- [ ] Leadership commitment documented: information security policy, roles, and resourcing
- [ ] Internal audit program established, with auditor independence from what's being audited
- [ ] Management review cadence established with documented outputs and actions
- [ ] Metrics defined for control effectiveness (you can show the ISMS is working, not just existing)
- [ ] Certification body selected; Stage 1 and Stage 2 audits scheduled

Score Yourself

Your result	What it means	Do this next
Audit-Ready (80%+ checked)	You're closer than most. Remaining gaps are findings waiting to happen.	Close the last gaps, then schedule the audit while momentum is high.
Foundation Built (50–79% checked)	Real progress, real exposure. This is where most companies stall for a year.	Prioritize unchecked items by deal impact. A readiness sprint beats a slow drift.
At Risk (under 50% checked)	An audit today would hurt. More importantly, so would an incident.	Don't buy an audit yet. Start with the Universal Core, it's a Tuesday afternoon, not a six-figure engagement.

Three Mistakes That Make Compliance Expensive

Buying the audit before the readiness. A failed or stalled audit costs more than preparation ever would.

Scoping too big. Whether it's CUI boundaries or ISMS scope, everything you include is something you must defend.

Treating it as a project instead of a program. Compliance you rebuild from scratch every year costs 3x compliance you maintain.

Want a second set of eyes on your unchecked boxes?
I do a free 20-minute readiness gut-check, useful whether we ever work together or not. DM me on LinkedIn (linkedin.com/in/aliallage) or visit **bluesteelcyber.com**.

Ali Allage, CEO, BlueSteel Cybersecurity | CMMC Registered Practitioner

This checklist is general guidance, not legal advice. Framework requirements vary by contract, data, and regulator.