NovaGRC

WHITE PAPER

Framework Selection Guide: SOC 2, ISO 27001 & NIST CSF

A practical decision framework for consultants advising clients on which compliance framework to pursue first — and how to sequence multiple frameworks efficiently.

Published August 2026

novagrc.com

Executive Summary

One of the most common questions vCISOs and compliance consultants face is: "Which framework should we start with?" The answer depends on the client's industry, customer base, regulatory environment, and growth trajectory — but the decision is often made based on incomplete information or sales pressure from audit firms.

This guide provides a structured decision framework for advising clients on framework selection, covering the three most commonly requested standards — SOC 2 Type II, ISO 27001, and NIST Cybersecurity Framework (CSF) 2.0 — along with considerations for HITRUST and HIPAA. We examine the strategic rationale for each, how they overlap, and how to sequence multi-framework programs without duplicating effort.

Understanding the Three Pillars

SOC 2 Type II

SOC 2 is the de facto compliance standard for SaaS companies and technology service providers selling to US enterprises. Developed by the AICPA, it evaluates an organization against five Trust Services Criteria: Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Best for: SaaS companies, cloud service providers, data processors, and any business where enterprise customers require a compliance report as part of vendor due diligence.

Key characteristics:

- Attestation-based (issued by a CPA firm, not a certification body).
- Type I evaluates design at a point in time; Type II evaluates operating effectiveness over a period (typically 6–12 months).
- Flexible — organizations define their own controls as long as they satisfy the Trust Services Criteria.
- US-centric, though increasingly recognized globally.
- Audit cost: $30K–$100K+ depending on scope and auditor.

ISO 27001:2022

ISO 27001 is the international gold standard for information security management systems (ISMS). Unlike SOC 2's attestation model, ISO 27001 results in a formal certification issued by an accredited certification body.

Best for: Companies with international customers, organizations in regulated industries, government contractors, and businesses targeting European or APAC markets.

Key characteristics:

- Certification-based (3-year cycle with annual surveillance audits).
- Prescriptive control set (93 controls in Annex A of the 2022 revision).
- Requires a formal ISMS with documented policies, risk assessment methodology, and management review process.
- Globally recognized — often a prerequisite for international enterprise sales.
- Certification cost: $15K–$60K for initial audit, plus annual surveillance fees.

NIST Cybersecurity Framework (CSF) 2.0

NIST CSF is not a certification or attestation — it's a voluntary framework that provides a common language for managing cybersecurity risk. The 2.0 revision (released February 2024) added a sixth function (Govern) and expanded guidance for supply chain and organizational governance.

Best for: Organizations building a security program from scratch, US government contractors and subcontractors, critical infrastructure operators, and companies that need a risk management framework without the overhead of a formal audit.

Key characteristics:

- No audit or certification — used for internal maturity assessment and improvement.
- Six functions: Govern, Identify, Protect, Detect, Respond, Recover.
- Tiered implementation levels (Partial → Risk Informed → Repeatable → Adaptive).
- Free and publicly available — no licensing fees.
- Increasingly used as a baseline that maps to other frameworks.

The Decision Framework

When advising clients on framework selection, work through these four decision factors in order:

1. Customer Requirements (Demand-Driven)

The most powerful driver is what customers are actually asking for. If enterprise prospects are requesting a SOC 2 report during sales cycles, that's your answer — the framework is dictated by the market.

Customer Profile	Likely Requirement	Recommended Framework
US enterprise SaaS buyers	SOC 2 Type II report	SOC 2
European/APAC enterprises	ISO 27001 certificate	ISO 27001
US federal agencies	NIST-aligned security program	NIST CSF + 800-53
Healthcare organizations	HIPAA compliance evidence	HITRUST or HIPAA + SOC 2
No specific requirement	General security posture	NIST CSF (then add certifications)

2. Regulatory Environment

Some frameworks are mandated by regulation or strongly implied by industry standards. Healthcare organizations handling PHI need HIPAA compliance. Financial services firms may need SOC 2 plus specific regulatory controls. Defense contractors need NIST 800-171 / CMMC.

3. Geographic Footprint

ISO 27001's international recognition makes it the default choice for companies with significant non-US operations or customer bases. SOC 2 is primarily a US standard, though it's gaining traction in other markets. NIST CSF is US-originated but framework-agnostic enough to work globally.

4. Organizational Maturity

For organizations with no existing security program, starting with NIST CSF as an internal maturity framework, then layering on SOC 2 or ISO 27001 for external credibility, is often the most efficient path.

> **Consultant's Rule of Thumb:** If the client's sales team is losing deals because they can't produce a compliance report, start with whatever framework the buyers are requesting. Everything else is secondary to revenue impact.

Framework Overlap: The Efficiency Opportunity

The good news for consultants managing multi-framework programs: there is substantial overlap between SOC 2, ISO 27001, and NIST CSF. A well-designed GRC program can satisfy multiple frameworks with a single set of controls, mapped across frameworks.

Control Overlap Analysis

Control Domain	SOC 2	ISO 27001	NIST CSF
Access Control	CC6.1–CC6.3	A.8, A.9	PR.AA, PR.AC
Risk Assessment	CC3.1–CC3.4	6.1, 8.2–8.3	GV.RM, ID.RA
Incident Response	CC7.3–CC7.5	A.5.24–A.5.28	RS.AN, RS.MI
Change Management	CC8.1	A.8.32	PR.IP
Vendor Management	CC9.2	A.5.19–A.5.22	GV.SC
Business Continuity	A1.1–A1.3	A.5.29–A.5.30	RC.RP

By implementing controls once and mapping them across frameworks, a consultant can deliver SOC 2 + ISO 27001 readiness with roughly 30–40% less effort than pursuing each independently.

Cross-Mapping Strategy

The most efficient approach is to use a unified control set — implement each control once, then map it to the relevant requirements in each framework. This requires a GRC platform that supports multi-framework mapping rather than maintaining separate compliance plans per framework.

Sequencing Multi-Framework Programs

For clients pursuing multiple frameworks, sequencing matters. Here are the three most common paths:

Path A: SOC 2 First → ISO 27001

Best for US SaaS companies expanding internationally. Start with SOC 2 Type II (6–12 month observation period), then layer ISO 27001 on top. ~60% of SOC 2 controls map directly to ISO 27001 Annex A requirements.

Path B: NIST CSF Foundation → SOC 2 or ISO 27001

Best for organizations building from scratch. Use NIST CSF to establish baseline security governance, then pursue formal certification/attestation once the program is mature. This avoids the "audit-driven" trap where controls are implemented hastily to pass an audit rather than to manage risk.

Path C: ISO 27001 First → SOC 2

Best for international companies entering the US market. ISO 27001's structured ISMS provides a strong foundation that SOC 2 controls map onto efficiently.

Practical Recommendations for Consultants

1. **Lead with the business case.** Frame compliance as a revenue enabler (closing enterprise deals, entering new markets) rather than a cost center.
2. **Build the risk program first.** Regardless of which framework you're targeting, a solid risk register is the foundation everything else maps to.
3. **Use cross-mapping from day one.** Even if the client only needs SOC 2 today, structure your controls so they can map to ISO 27001 later without rework.
4. **Invest in templates.** Develop reusable, industry-specific control templates that you can deploy across clients — this is where your practice's IP lives.
5. **Automate evidence collection.** The ongoing cost of compliance is evidence management, not the initial assessment. Build evidence workflows early.

Conclusion

Framework selection shouldn't be a guessing game. By working through customer requirements, regulatory environment, geographic footprint, and organizational maturity in that order, consultants can provide clear, defensible recommendations that align compliance investment with business value.

The most impactful advice you can give a client isn't "get SOC 2" or "get ISO 27001." It's "here's the sequence that gets you to audit-ready with the least duplicated effort, while building a risk management program that actually makes your business more resilient."