ControlSage

Security Compliance Frameworks Compared

SOC 2 · ISO 27001 · HIPAA · PCI DSS · GDPR · NIST — a practical guide for IT and security professionals evaluating which framework fits their business.

Why Framework Selection Is a Strategic Decision

Wrong Framework = Wasted Spend

Average compliance programs cost **$500K–$2M+ annually**. Choosing the wrong framework burns budget without delivering business value.

Right Framework = Competitive Edge

Faster enterprise sales cycles, reduced breach liability, and stronger vendor trust — compliance done right is a **revenue enabler**.

Overlap Reduces Redundant Effort

Most organizations need **2–3 overlapping frameworks**. Understanding control overlap reduces redundant effort by **30–40%**.

CHAPTER 1 OF 3

Framework Profiles

A deep dive into each of the six major security and privacy frameworks — who they apply to, what they cover, and how they're enforced.

SOC 2

The SaaS & Cloud Standard

- **Who it applies to:** US-based SaaS, cloud, and managed service providers handling customer data
- **Scope:** 5 Trust Service Criteria — Security, Availability, Confidentiality, Processing Integrity, Privacy
- **Type I** (point-in-time) vs **Type II** (6–12 month audit) — enterprise buyers almost always require Type II
- **Enforcement:** No legal mandate; market-driven — increasingly required in B2B contracts

ISO 27001

The Global ISMS Standard

- **Who it applies to:** Any organization globally; dominant in Europe, APAC, and government procurement
- **Scope:** 93 controls across 4 themes — Organizational, People, Physical, Technological
- **Certification:** Issued by accredited third-party bodies; valid 3 years with annual surveillance audits
- **Enforcement:** No direct legal penalty; required for many EU/UK government and enterprise contracts

ISO 27001 is the most internationally recognized ISMS certification — a strong baseline for global market entry.

HIPAA

Healthcare Data Protection

Who It Covers

US healthcare providers, insurers, clearinghouses, and all business associates (BAs) touching ePHI

Three Core Rules

Privacy Rule · Security Rule · Breach Notification Rule

Key Controls

Access controls, audit logs, encryption, and BAAs with every vendor handling ePHI

Enforcement

OCR fines up to **$1.9M per violation category/year**; criminal penalties possible

PCI DSS

Payment Card Security

- **Who it applies to:** Any entity that stores, processes, or transmits cardholder data — globally
- **Scope:** 12 requirements across 6 goals — network security, access control, monitoring, and more
- **Version:** PCI DSS v4.0 (2024) adds customized implementation and enhanced MFA requirements
- **Enforcement:** Card brand fines of **$5K–$100K/month**, increased transaction fees, or loss of card processing rights

GDPR

EU Privacy Regulation

Global Reach

Applies to **any organization** processing personal data of EU/EEA residents — regardless of where the org is based

Core Scope

Lawful basis for processing, data subject rights, DPIAs, and 72-hour breach notification window

Key Roles

Data Controller vs Data Processor — each carries distinct obligations under the regulation

Max Penalties

Fines up to **€20M or 4% of global annual turnover** — whichever is higher

NIST CSF & SP 800-53

The US Federal Baseline

- **Who it applies to:** US federal agencies (mandatory); widely adopted by critical infrastructure and defense contractors
- **NIST CSF 2.0:** 6 functions — Govern, Identify, Protect, Detect, Respond, Recover
- **SP 800-53:** 20 control families; required for FedRAMP, FISMA, and DoD contracts (CMMC maps to it)
- **Enforcement:** Mandatory for federal systems; voluntary but contractually required for government vendors

CHAPTER 2 OF 3

Side-by-Side Comparison

Applicability, cost, key requirements, and penalties — all six frameworks evaluated on the dimensions that matter most to your decision.

Applicability & Geography

Framework	Geography	Primary Sector	Mandatory?
SOC 2	US (global recognition)	SaaS / Cloud	No (market-driven)
ISO 27001	Global	Any industry	No (contract-driven)
HIPAA	US	Healthcare	Yes (legal)
PCI DSS	Global	Payments	Yes (contractual)
GDPR	EU/EEA + global reach	Any (EU data)	Yes (legal)
NIST	US	Federal / Gov contractors	Yes (federal)

Key Requirements at a Glance

SOC 2

Policies, logical access, change management, incident response, availability monitoring

ISO 27001

Risk assessment, ISMS documentation, 93 Annex A controls, management review

HIPAA

PHI access controls, encryption, audit logs, BAAs, workforce training

PCI DSS

Network segmentation, cardholder data encryption, vulnerability scanning, pen testing

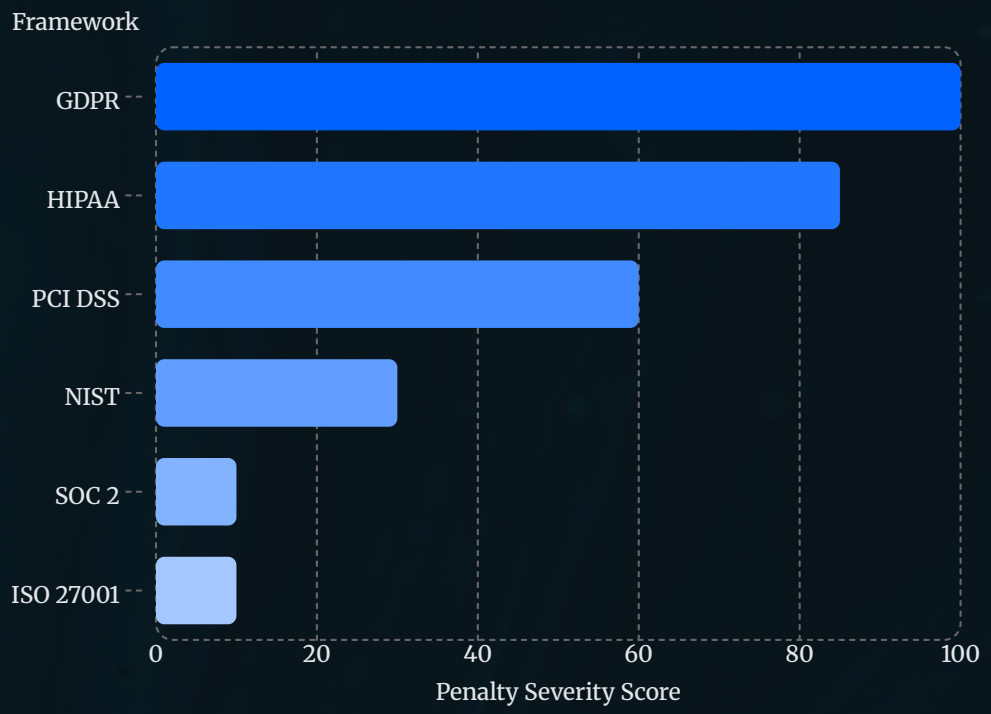
GDPR

Consent management, DPIAs, data subject request workflows, DPA agreements

NIST

Asset inventory, continuous monitoring, incident response, supply chain risk management

Penalties & Enforcement Compared



What the Numbers Mean

GDPR carries the steepest statutory fines — €20M or 4% of global annual revenue, whichever is higher.

HIPAA follows closely with OCR fines up to $1.9M per violation category per year and criminal exposure for willful neglect.

PCI DSS enforcement is contractual: card brands levy $5K–$100K/month in fines or revoke processing rights entirely.

NIST, SOC 2, and ISO 27001 carry no direct statutory fines — but non-compliance means lost contracts, failed audits, and market exclusion.

Framework Overlap & Synergies

SOC 2 + ISO 27001

~60% control overlap — pursue together to satisfy US and global buyers simultaneously and maximize audit ROI

HIPAA + NIST SP 800-66

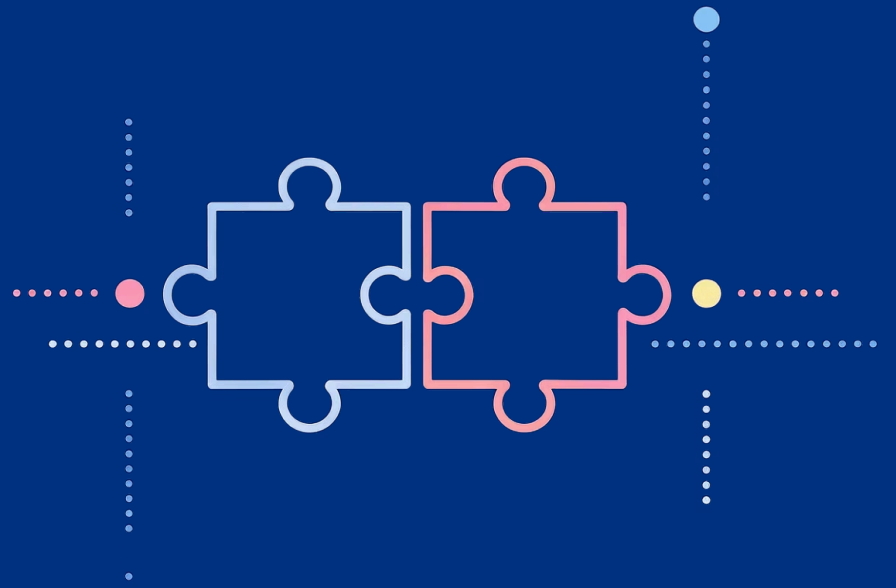
NIST provides the authoritative implementation guide for HIPAA Security Rule controls — natural pairing for health-tech

PCI DSS + SOC 2

Shared controls in access management, logging, and encryption significantly reduce the dual-audit burden

GDPR + ISO 27001

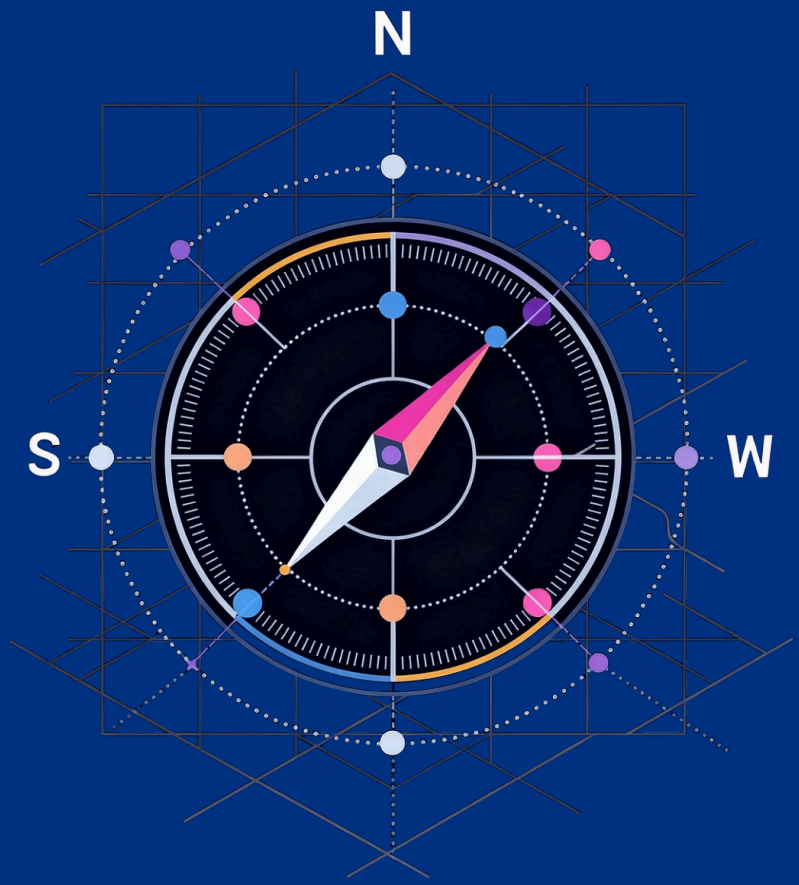
ISO 27701 (the privacy extension) maps directly to GDPR requirements — one ISMS to cover both



CHAPTER 3 OF 3

Decision Guide

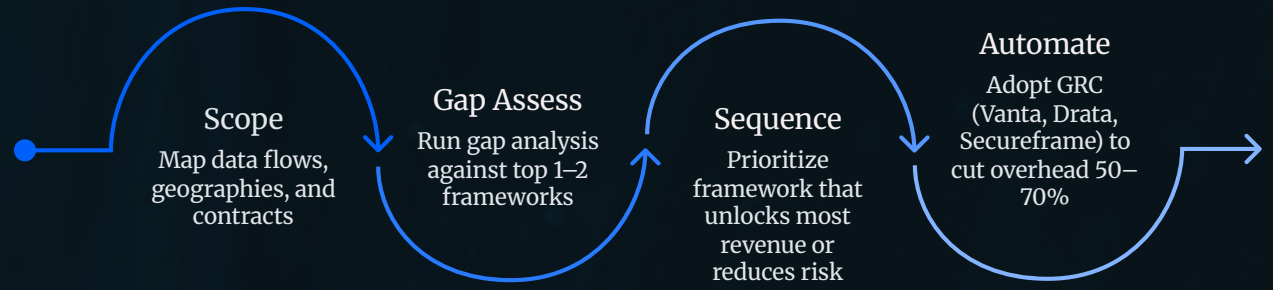
Use the profiles and comparisons to select the right starting point — then build a sequenced roadmap that unlocks revenue and reduces risk.



Which Framework Fits Your Business?

If you are…	Start with…	Also consider…
A US SaaS company selling to enterprise	**SOC 2 Type II**	ISO 27001 for global expansion
A global company or EU market entrant	**ISO 27001**	GDPR (if handling EU personal data)
A healthcare provider or health-tech startup	**HIPAA**	SOC 2 (if you're a BA/SaaS)
An e-commerce or fintech handling card payments	**PCI DSS**	SOC 2 or ISO 27001
A US federal contractor or DoD supplier	**NIST SP 800-53 / CMMC**	FedRAMP (if cloud services)
Any company with EU customers	**GDPR**	ISO 27001 + ISO 27701

Your Compliance Roadmap: Next Steps



Most organizations can complete Steps 1 and 2 in 4–6 weeks with existing staff. Step 4 automation typically delivers **50–70% reduction** in ongoing compliance overhead — making it the highest-ROI investment in your compliance program.