



AEGIS

COMPLIANCE

Compliance Framework Reference

Quick reference for FedRAMP, StateRAMP, SOC 2, HIPAA, and other compliance frameworks



FedRAMP



SOC 2



HIPAA



PCI DSS

Framework Overview

Framework	Scope	Who Needs It	Timeline
FedRAMP	Federal cloud security	Federal contractors	12-18 months
StateRAMP	State/local cloud security	State contractors	6-12 months
SOC 2 Type II	Service org controls	SaaS, cloud services	6-12 months
HIPAA	Healthcare data	Healthcare providers	6-9 months
PCI DSS	Payment card data	Payment processors	6-12 months
ISO 27001	InfoSec management	International orgs	6-12 months
CMMC	Defense contractor security	DoD contractors	12-18 months

FedRAMP Impact Levels

Low Impact

~125 controls
Public info systems
Minimal disruption if breached

Moderate Impact

~325 controls
Most common level
Serious adverse effects

High Impact

~421 controls
National security data
Catastrophic effects

SOC 2 Trust Service Criteria

Category	Focus Area	Key Controls
Security (CC)	Protection from unauthorized access	Access controls, encryption, monitoring
Availability (A)	System uptime commitments	SLAs, DR, capacity planning
Processing Integrity (PI)	Data processing accuracy	Quality controls, error handling
Confidentiality (C)	Protection of sensitive data	Encryption, access limits, DLP
Privacy (P)	Personal data handling	Consent, retention, disclosure

HIPAA Requirements

Administrative Safeguards

- Security management process
- Workforce security
- Information access management
- Security awareness training
- Contingency plan

Technical Safeguards

- Access controls
- Audit controls
- Integrity controls
- Transmission security
- Authentication



Get Compliance Ready

Our experts can help you achieve and maintain compliance with any framework. Start with a gap assessment.

Contact Us

 info@aegisit.ai

 (404) 490-0234

 aegisit.ai