GRC+ DIGEST · 21 NOVEMBER 2026

United States Digest

What applies in the United States, and by when. Each requirement with its dates, supervisors, incident deadlines and fines; then how GRC+ helps.

Coming Up

DATE	REQUIREMENT	WHAT HAPPENS
31 Dec 2026		Swift CSP attestation due
15 Apr 2027	NYDFS Part 500	Deadline for the annual certification or acknowledgment

Three Requirements to Look at First

LAW · APPLIES SINCE 1 MARCH 2017

NYDFS Part 500

Key dates **1 Nov 2025** Last phase: universal multi-factor authentication and asset inventory
15 Apr 2027 Deadline for the annual certification or acknowledgment (coming up)

LAW · APPLIES SINCE 20 APRIL 2005

HIPAA

Key dates **6 Jan 2025** Proposed update published

LAW · APPLIES SINCE 18 DECEMBER 2023

SEC cyber rules

Key dates **15 Jun 2024** Applies to smaller reporting companies
Supervisors SEC

The First Three in Detail

LAW · APPLIES SINCE 1 MARCH 2017

NYDFS Part 500

Requires DFS-regulated banks, insurers and financial services firms to run a risk-based cybersecurity programme and certify compliance each year.

Key dates	**1 Mar 2017** Part 500 takes effect **1 Nov 2025** Last phase: universal multi-factor authentication and asset inventory **15 Apr 2027** Deadline for the annual certification or acknowledgment (coming up)
How we help	NYDFS Part 500 Cybersecurity Audit

LAW · APPLIES SINCE 20 APRIL 2005

HIPAA

Requires US health plans, providers, clearinghouses and their business associates to protect electronic health information based on a risk analysis.

Key dates	**20 Apr 2005** Compliance required **6 Jan 2025** Proposed update published
How we help	CISO as-a-Service

LAW · APPLIES SINCE 18 DECEMBER 2023

SEC cyber rules

Requires US public companies to disclose material cybersecurity incidents on Form 8-K and describe cyber risk governance in Form 10-K.

Key dates	**15 Dec 2023** Annual cyber disclosure starts **18 Dec 2023** Form 8-K incident disclosure applies **15 Jun 2024** Applies to smaller reporting companies
Supervisors	Securities and Exchange Commission (SEC) Supervisory authority
How we help	CISO as-a-Service

Every Other Requirement in United States

The other requirements on the country page, with their status and the facts we have reviewed.

LAW · IN FORCE SINCE 1 APRIL 2022

12 CFR 53, 225, 304

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · IN FORCE SINCE 1 SEPTEMBER 2023

12 CFR 748

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · APPLIES SINCE 20 AUGUST 1997

21 CFR Part 11

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · APPLIES FROM 26 JANUARY 2027

A5175-A

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · APPLIES SINCE 1 JANUARY 2020

CCPA

Gives California residents rights to know, delete, correct and opt out of the sale or sharing of their personal information.

Key dates	**1 Jan 2020** CCPA in force **1 Jan 2027** ADMT requirements apply (coming up) **1 Apr 2028** Risk assessment attestations and the largest businesses' audit certifications due (coming up)
Supervisors	California Privacy Protection Agency Data protection authority
How we help	Outsourced DPO Service

LAW · ADOPTED

CIRCIA

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · APPLIES IN STAGES

CMMC

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · IN FORCE

Communications Act

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · IN FORCE SINCE 1 AUGUST 2026

Delete Act

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · IN FORCE

DFARS 252.204-7012

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · IN FORCE

EFTA

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · IN FORCE SINCE 21 MARCH 2019

FASCSA

The Federal Acquisition Supply Chain Security Act of 2018 set up the Federal Acquisition Security Council and allows exclusion and removal orders against sources and covered articles that pose supply chain risk to federal information systems.

Key dates	**21 Mar 2019** Takes effect, 90 days after enactment under section 205
How we help	Vendor Risk Management

LAW · APPLIES SINCE 29 MARCH 2023

FDA 524B

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · APPLIES SINCE 21 AUGUST 1974

FERPA

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · APPLIES SINCE 18 DECEMBER 2014

FISMA

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · APPLIES FROM 18 JANUARY 2027

GENIUS Act

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · APPLIES SINCE 12 NOVEMBER 1999

GLBA

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · APPLIES SINCE 14 APRIL 2003

HIPAA Privacy Rule

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · APPLIES SINCE 17 FEBRUARY 2009

HITECH Act

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · ADOPTED

NIST IR 8547

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · ADOPTED

NIST SP 800-108

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · ADOPTED

NIST SP 800-221

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · ADOPTED

NIST SP 800-82

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · IN FORCE

ONC Certification

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · APPLIES FROM 1 JANUARY 2027

RAISE Act

The RAISE Act is New York State law on frontier AI models (General Business Law Article 44-B). Frontier developers must publish transparency reports and report critical safety incidents within 72 hours. Large frontier developers must also publish a frontier AI framework and file a disclosure statement.

Key dates	**27 Mar 2026** Chapter 96 of 2026 signed, replacing Article 44-B **1 Jan 2027** RAISE Act requirements for large frontier AI developers take effect (coming up)
How we help	AI Governance Officer as-a-Service

LAW · IN FORCE

Regulation S-P

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · APPLIES FROM 1 JANUARY 2027

S9051-B

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · APPLIES SINCE 9 JUNE 2023

Safeguards Rule

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · APPLIES FROM 1 JANUARY 2027

SB26-189

Colorado SB26-189 repeals and re-enacts the 2024 AI law (SB24-205) with duties on automated decision-making technology in consequential decisions. Developers must give deployers documentation. Deployers must give notice, adverse outcome disclosures and human review.

Key dates	**14 May 2026** Signed by the Governor **1 Jan 2027** Takes effect (coming up)
How we help	AI Governance Officer as-a-Service

LAW · APPLIES SINCE 30 JULY 2002

SOX 404 and ITGC

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · IN FORCE

TPRM Guidance

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · APPLIES SINCE 16 JANUARY 2026

TSA Security Directives

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

LAW · IN FORCE SINCE 29 AUGUST 2024

USCTM

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

STANDARD · IN FORCE

CJIS Security Policy

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

STANDARD · APPLIES IN STAGES

FedRAMP

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

STANDARD · IN FORCE

FFIEC IT Handbook

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

STANDARD · APPLIES SINCE 14 MAY 2024

NIST SP 800-171

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

STANDARD · APPLIES SINCE 23 SEPTEMBER 2020

NIST SP 800-53

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

STANDARD · APPLIES SINCE 14 FEBRUARY 2024

NIST SP 800-66

Not yet reviewed: our review of this requirement is still open, so its facts are not in this digest.

Requirements by Sector

SECTOR	REQUIREMENTS	STANDARDS	SUPERVISORS
Financial Services and Insurance	12 CFR 53, 225, 304, 12 CFR 748, EFTA, GENIUS Act, GLBA, NYDFS Part 500, Regulation S-P, Safeguards Rule	FFIEC IT Handbook, NIST SP 800-66, Swift CSP, PCI DSS, HITRUST	FRB, CFTC, CFPB, FDIC, NCUA, DFS
Technology and Telecom	Communications Act, RAISE Act, S9051-B, Delete Act, NIST SP 800-108, NIST SP 800-221, NIST IR 8547, CCPA	CJIS Security Policy, FedRAMP, NIST SP 800-53, GSMA NESAS, ISO 22301	FCC
Healthcare and Life Sciences	21 CFR Part 11, FDA 524B, HIPAA Privacy Rule, HITECH Act, ONC Certification, HIPAA, CCPA, SB26-189	NIST SP 800-66, HITRUST, ISO 27799, SOC 2, IEC 80001-1	FDA, OCR
Public Sector and Defence	FASCSA, FERPA, FISMA, CMMC, DFARS 252.204-7012, NIST IR 8547, NIST SP 800-221, SB26-189	CJIS Security Policy, FedRAMP, NIST SP 800-171, NIST SP 800-53, ISO 27001	
Manufacturing and Chemicals	USCTM, A5175-A, NIST SP 800-82, NIST SP 800-108	IEC 62443, ISO 27001, NIST CSF, ETSI EN 303 645, IACS UR E26/E27	

Automotive and Transportation	TSA Security Directives, CIRCIA, SEC cyber rules, SOX 404 and ITGC	TISAX, ISO/SAE 21434, ISO 27001, NIST CSF, ISO 24089	TSA
Energy and Utilities	NIST SP 800-82, TSA Security Directives, CIRCIA, SEC cyber rules, SOX 404 and ITGC	IEC 62443, ISO 27001, IEC 62351, ISO/IEC 27019, CIS Controls	FERC, NRC, TSA
Aviation and Space	CMMC, DFARS 252.204-7012, SEC cyber rules, SOX 404 and ITGC	NIST SP 800-171, ISO 27001, ED-202A / DO-326A, ISO 9001, ISO 31000	FAA, TSA
Retail, Consumer and Leisure	A5175-A, Delete Act, CCPA, SEC cyber rules, SOX 404 and ITGC	PCI DSS, ETSI EN 303 645, ISO/IEC 27701, NIST Privacy Framework, CIS Controls	FDA

Who Supervises

SUPERVISOR	SUPERVISES	WEBSITE
Securities and Exchange Commission SEC	SEC cyber rules	sec.gov/about
California Privacy Protection Agency	CCPA	cppa.ca.gov

How GRC+ Helps

We never audit work our own team runs for you. A team of four to five practitioners, under one contract for every country you operate in.

Stay Compliant
Ongoing work: pay as you go or monthly.

Incident Reporting Desk
Vendor Risk Management
EU and UK Representative
CISO as-a-Service
Outsourced DPO Service
AI Governance Officer as-a-Service
Compliance Officer as-a-Service
Internal Audit as-a-Service
Government Relations as-a-Service

Audit or Assess An independent view, because a regulation requires one or because you want to know for yourself. We never audit a role our own team runs for you.	NYDFS Part 500 Cybersecurity Audit Stablecoin Reserve Controls Readiness Review Swift CSP Assessment ISO 27001 Internal Audit NIS2 Compliance Assessment DORA Compliance Audit Data Protection Compliance Audit PCI DSS Readiness Assessment EU AI Act Readiness Assessment SOC 2 and Assurance Report Review DSA Compliance Review IEC 62443 Security Assessment MiCA Compliance Audit Security Maturity Assessment Post-Quantum Cryptography Readiness Assessment PSD2 SCA Audit Security Architecture Review Cyber Resilience Act Readiness Assessment ISO 42001 Internal Audit ISO 27701 Internal Audit Data Protection Impact Assessment (DPIA)
Build and Fix One-off work that closes the gaps.	NIS2 Readiness Programme DORA Gap Remediation AI Act Compliance Programme ISO 27001 Implementation Incident Response Plan and Exercise
Security Testing Tests that show whether attacks are detected and stopped.	Red Teaming Penetration Testing Cloud Security Assessment Source Code Review

Talk to Us

Thirty minutes with a principal consultant on what applies to you and what to do first.

Book a 30-Minute Call · sales@grc.plus · +1 (424) 363-4300

Dates and requirements come from the GRC+ regulation pages and change as they do. The latest version: grc.plus/us