ZenGRC

ZenGRC Simply Powerful GRC

GUIDE · FRAMEWORK MAPPING

Multi-Framework Control Mapping Guide

Where your frameworks overlap. Where they diverge. How to use it.
Based on 4,214 framework program instances in ZenGRC.

Source
4,214 program instances

Frameworks
SOC 2, ISO 27001, HIPAA, HITRUST, NIST, PCI

Published
2026 · ZenGRC

FRAMEWORK PAIRING 01

SOC 2 + ISO 27001

The most common pairing. The highest overlap.

~80%
Control overlap between frameworks

534
SOC 2 program instances in ZenGRC

~20%
Net new controls when adding ISO 27001

SHARED CONTROLS

Access management, encryption, change management, incident response, risk assessment, vendor management, business continuity, monitoring and logging.

SOC 2 ONLY

Trust Services Criteria for availability, processing integrity, and confidentiality as distinct categories.

ISO 27001 ONLY

Annex A with 93 controls, mandatory management review, internal audit program, formal ISMS documentation.

ADDING ISO 27001 TO SOC 2

Approximately 20% additional controls, primarily formal ISMS structure and Annex A specifics.

💡 **Takeaway**

If you run SOC 2, you are 80% of the way to ISO 27001. Map once. Test once. Apply to both.

FRAMEWORK PAIRING 02

HIPAA + HITRUST

The healthcare compliance pairing.

360
HITRUST r2 requirement statements

100%
HIPAA Security Rule covered by HITRUST

60+
Standards harmonized within HITRUST

SHARED CONTROLS

Access controls, encryption, audit logging, incident response, risk assessment, workforce training, backup and recovery.

HIPAA ONLY

Privacy Rule (data use, disclosure, minimum necessary, patient rights), Breach Notification, 6-year retention.

HITRUST ONLY

Maturity scoring across policy, procedure, and implementation. 14 control categories harmonizing 60+ standards, interim assessments.

THE TWO-WORLDS PROBLEM

HIPAA often sits with legal/privacy. HITRUST sits with infosec. Different people, different processes — but overlapping requirements.

💡 **Takeaway**

HITRUST covers all HIPAA Security Rule requirements. Bridge the two teams. Eliminate the duplicate work.

FRAMEWORK PAIRING 03

SOC 2 + NIST CSF

Voluntary framework pairing with strong alignment.

~70%
Control alignment between frameworks

5+5
SOC 2 Trust Services Criteria + NIST categories

~30%
Net new controls when adding NIST CSF

SHARED CONTROLS

Access management, data protection, incident response, vulnerability management, change management, logging, vendor risk.

SOC 2 ONLY

Trust Services Criteria structure, formal CPA audit opinion, Type I vs. Type II distinction.

NIST CSF ONLY

Identify-Protect-Detect-Respond-Recover structure, supply chain risk emphasis, governance tier maturity model.

ADDING NIST CSF TO SOC 2

Approximately 30% additional controls for identification, recovery planning, and supply chain risk management.

💡 **Takeaway**

NIST fills the risk identification gaps SOC 2 leaves open. A strong pairing for companies adding structure to their program.

FRAMEWORK PAIRING 04

PCI DSS + SOC 2

The retail and payments pairing.

296
PCI program instances in ZenGRC

~60%
Control overlap with SOC 2

~40%
Net new controls when adding PCI DSS

SHARED CONTROLS

Access controls, encryption, network security, logging, vulnerability management, incident response, vendor management.

PCI DSS ONLY

Cardholder data scoping, network segmentation, quarterly ASV scans, PCI DSS 4.0 authentication requirements.

SOC 2 ONLY

Broader trust services criteria, availability and processing integrity, flexible control design.

ADDING PCI DSS TO SOC 2

Approximately 40% additional controls for cardholder data handling, network segmentation, and scanning requirements.

💡 **Takeaway**

PCI has the most prescriptive requirements — but 60% of the work is already done if you have SOC 2.

REFERENCE

The Overlap Matrix

How much new work each framework adds.

STARTING WITH	ADDING	OVERLAP	NET NEW	EFFORT
SOC 2	ISO 27001	~80%	~20%	Low
SOC 2	NIST CSF	~70%	~30%	Low
SOC 2	HIPAA	~65%	~35%	Med
SOC 2	PCI DSS	~60%	~40%	Med
HIPAA	HITRUST	~85%*	~15%	Low
ISO 27001	SOC 2	~80%	~20%	Low
NIST 800-171	CMMC L2	~90%	~10%	Low

** HITRUST incorporates HIPAA Security Rule by design. All percentages are approximate.*

💡 **The Big Insight**

Every framework after the first has 60–90% overlap. The work is in finding the net new — not retesting the shared.

ZenGRC

Test once.
Apply everywhere.

Stop Testing the Same Controls Twice.

ZenGRC maps controls across frameworks automatically. Collect evidence once. Reuse across audits. One platform, unlimited users, unlimited frameworks — one price.

Request a Demo →

zengrc.com/demo