// TMG SECURITY RESEARCH — COMPARISON GUIDE

# ISO 27001 vs SOC 2 vs PCI DSS: Comparison Guide

A side-by-side comparison of what each framework actually asks, what it produces, and how organizations typically choose between them.

---

**TMG Security Research Team**

Version 1.0

Published 07 September 2026

External facts checked against ISO, AICPA and PCI Security Standards Council official sources

## Executive summary

ISO 27001, SOC 2 and PCI DSS are the three compliance frameworks organizations most often need to address, and they're frequently confused with one another despite asking fundamentally different questions and producing different outcomes. ISO/IEC 27001:2022 is a certification: an organization's information security management system is confirmed to meet the standard. SOC 2 is not a certification — it's an examination that produces an attestation report, evidencing that a service organization's controls operated as described. PCI DSS isn't optional in the way the other two are: it's a requirement, published and governed by the PCI Security Standards Council, for any organization that stores, processes or transmits payment card data.

This guide compares what each framework actually asks, what it produces, who typically pursues it, and how organizations often combine more than one. It's TMG Security's own comparison — built from the readiness work we do directly with clients, and checked against each framework's official published source — and it doesn't replace the official documentation for any of the three.

## Quick comparison

| Dimension | ISO 27001 | SOC 2 | PCI DSS |
|---|---|---|---|
| **What it is** | Standard specifying ISMS requirements. | AICPA reporting framework; examination producing an attestation report. | Global data security standard for payment card data. |
| **Primary focus** | Governance, risk treatment, managed controls over time. | Controls operating over a period, evidenced consistently. | Segmentation, cardholder data protection, technical controls. |
| **Who pursues it** | Orgs wanting ongoing governance structure. | Orgs selling to enterprise buyers needing evidence. | Any org storing/processing/transmitting card data. |
| **What it produces** | Certification to ISO/IEC 27001:2022. | A SOC 2 report (attestation, not certification). | Validated compliance (ROC or SAQ). |
| **Current version** | ISO/IEC 27001:2022 (3rd ed., Oct 2022; amended 2024) | 2017 TSC, 2022 revised points of focus | v4.0.1 (v3.2.1 retired Mar 31, 2024) |
| **Governing body** | ISO/IEC (JTC 1/SC 27) | AICPA | PCI Security Standards Council |
| **Structure** | Controls selected by risk, detailed in Annex A / ISO 27002. | 5 Trust Services Criteria: Security, Availability, Processing Integrity, Confidentiality, Privacy. | 12 requirements grouped into 6 goals. |

*ISO/IEC 27001's current Annex A control count and a SOC 2 Type I/Type II distinction were intentionally omitted — see Scope and limitations.*

// TMG SECURITY RESEARCH — COMPARISON GUIDE

# ISO 27001 vs SOC 2 vs PCI DSS

What each framework actually asks, what it produces, and how organizations typically choose between them.

TMG Security Research Team · v1.0 · Published 07 Sep 2026 · Facts checked against ISO, AICPA and PCI SSC official sources

AT A GLANCE

## What each framework is, and what it produces

### ISO 27001

ISO/IEC 27001:2022 · ISO/IEC

**WHAT IT IS**
An international standard specifying requirements for an information security management system (ISMS).

**PRIMARY FOCUS**
Governance, risk treatment and a managed set of controls reviewed over time.

**WHO PURSUES IT**
Organizations that want a recognised, ongoing security governance structure.

**WHAT IT PRODUCES**
Certification to ISO/IEC 27001:2022.

### SOC 2

2017 TSC, 2022 points of focus · AICPA

**WHAT IT IS**
An AICPA reporting framework — an examination of a service organization's controls, evidenced through an attestation report.

**PRIMARY FOCUS**
Controls operating over a period, evidenced consistently, usually for customer assurance.

**WHO PURSUES IT**
Organizations selling to enterprise buyers who ask for evidence rather than a badge.

**WHAT IT PRODUCES**
A SOC 2 report — an attestation, not a certification.

### PCI DSS

v4.0.1 · PCI Security Standards Council

**WHAT IT IS**
A global data security standard with technical and operational requirements for protecting payment card account data.

**PRIMARY FOCUS**
Segmentation, protection of cardholder data and tightly specified technical controls.

**WHO PURSUES IT**
Any organization that stores, processes or transmits payment card data.

**WHAT IT PRODUCES**
Validated compliance — a Report on Compliance (ROC) or Self-Assessment Questionnaire (SAQ).

HOW TO CHOOSE

## Quick decision guide

**WANT ONGOING GOVERNANCE**
ISO 27001 — a recognised, ongoing security management system, certified rather than reported.

**ENTERPRISE BUYERS ASKING FOR EVIDENCE**
SOC 2 — an attestation report showing controls actually operated as described.

**HANDLING CARD PAYMENTS**
PCI DSS — not optional. Required for any entity that stores, processes or transmits card data.

TMGSecurity

## ISO 27001 in detail

ISO/IEC 27001:2022 is the current edition of the international standard for information security management systems — the third edition, published by ISO/IEC in October 2022, with an amendment published in 2024. It specifies requirements an organization's information security management system (ISMS) must satisfy: governance, risk treatment, and a managed set of controls reviewed over time. Organizations that complete the process are described as certified to ISO/IEC 27001:2022.

TMG's own readiness work with clients typically surfaces the same considerations: scope definition, risk methodology, the Statement of Applicability, management review and internal audit. The standard's Annex A sets out the controls organizations select from based on risk, detailed further in ISO/IEC 27002:2022 — we've deliberately left the current control count out of this guide rather than repeat a figure we could not verify directly from ISO.

## SOC 2 in detail

SOC 2 sits within the AICPA's System and Organization Controls (SOC) suite of CPA service offerings, rather than being a standard an organization is certified against. The AICPA and the licensed firms that perform this work describe it as an examination that produces an attestation report — not a certification. It's built on the AICPA's Trust Services Criteria: Security, Availability, Processing Integrity, Confidentiality and Privacy, most recently the 2017 Trust Services Criteria with revised points of focus issued in 2022.

TMG's own readiness work for this framework typically covers criteria selection, control design, and evidence collection over the review period — the report's value comes from demonstrating that selected controls operated consistently, not from a one-time check.

## PCI DSS in detail

PCI DSS is a global standard, published and governed by the PCI Security Standards Council, providing a baseline of technical and operational requirements to protect payment card account data. It applies to entities that store, process, or transmit cardholder data and/or sensitive authentication data. The current version is v4.0.1 (v3.2.1 retired March 31, 2024), and the standard remains organized into 12 requirements grouped under 6 goals.

TMG's own readiness work for this framework typically covers scope reduction, network segmentation, key management, and logging and testing requirements. Depending on an organization's size and how it processes card data, compliance is validated through a Report on Compliance (ROC) prepared by a Qualified Security Assessor (QSA), or a Self-Assessment Questionnaire (SAQ).

## How to choose

These three frameworks answer different questions and are not interchangeable. ISO 27001 asks whether you are running a managed information security programme: it certifies a management system, not a point-in-time control set, and is usually chosen when an organization wants a recognised, ongoing security governance structure. SOC 2 asks whether your controls actually operated as described over a period of time: it produces a report for customer assurance rather than a certification, and is usually chosen when enterprise buyers are asking for evidence rather than a badge. PCI DSS is not a choice in the same sense — it is a requirement for any organization that stores, processes or transmits payment card data.

## Using more than one framework

In practice, organizations often need more than one: a SaaS company selling to enterprises frequently pursues SOC 2 for customer assurance while working toward ISO 27001 for its broader security programme, and any organization handling card payments needs PCI DSS regardless of what else it pursues. Which combination applies depends on your sector, your customers and where you operate.

## Scope and limitations

- TMG Security is not a certification body or auditor, and does not issue certifications, attestations, or audit opinions for ISO 27001, SOC 2, PCI DSS, or any other framework.
- This guide is educational and comparative. It reflects TMG's own comparison of these three frameworks, checked against official sources at the time of publication — it is not legal, regulatory, audit or certification advice.
- Official framework documentation always takes precedence over this guide. Consult ISO, the AICPA, and the PCI Security Standards Council directly for authoritative, current requirements.
- Standards and frameworks are revised over time — this guide reflects ISO/IEC 27001:2022, SOC 2's 2017 Trust Services Criteria (2022 points of focus), and PCI DSS v4.0.1 as of the publication date above. Verify the current published version before relying on specific requirements.
- Two details were deliberately left out because TMG could not confirm them from an official source at publication: ISO/IEC 27001:2022's current Annex A control count, and a formal SOC 2 Type I / Type II distinction.

## References


### TMG SOURCES

- tmgsec.com/grc-compliance/
- tmgsec.com/iso-27001-soc2-pci-dss/

### OFFICIAL EXTERNAL SOURCES

- ISO/IEC 27001:2022 — iso.org/standard/27001
- AICPA & CIMA — SOC 2 / Trust Services Criteria
- PCI Security Standards Council — PCI DSS


> **This is TMG Security's own comparison guide.** TMG does not create, govern, certify, attest to, or audit against ISO 27001, SOC 2, or PCI DSS, and is not affiliated with ISO, the AICPA, or the PCI Security Standards Council. TMG Security is not a certification body or auditor and does not issue certifications or audit opinions.