tufin

Audit-Prep Checklist

What Auditors Ask About Segmentation

Almost every major compliance framework expects you to keep sensitive systems separated from the rest of your network, and to prove it. Use this checklist before your next audit to see where you stand. Each box you can't tick yet is a question to be ready for.

PCI DSS

v4.0.1 · Requirements 1, 11.4.5–11.4.6, 12.5.2

- [ ] Can you show exactly which systems are inside your cardholder data environment, and which are not?
- [ ] Has segmentation been tested in the last 12 months (6 months for service providers) and after every change to it?
- [ ] Can you show that only necessary traffic reaches the cardholder data environment?

HIPAA Security Rule

45 CFR §164.308 and §164.312

- [ ] Does your risk analysis cover who and what can reach systems holding patient data (ePHI)?
- [ ] Do access controls limit network access to ePHI to only what each role needs?
- [ ] Are you tracking the proposed Security Rule update, which would make network segmentation an explicit requirement?

NIST

CSF 2.0 PR.IR-01 · SP 800-53 SC-7, AC-4

- [ ] Are networks divided by trust level, with only necessary traffic allowed between them?
- [ ] Are key internal boundaries controlled and monitored, not just the outer perimeter?
- [ ] Can you show how traffic between zones is enforced?

ISO/IEC 27001

2022 · Annex A 8.20, 8.22

- [ ] Are groups of systems, users, and services separated into networks or zones?
- [ ] Is the reason for each zone documented, along with the traffic allowed between zones?
- [ ] Do you review your zones regularly to confirm they still match the design?

SOC 2

Trust Services Criteria CC6.1, CC6.6

- [ ] Can you show logical access controls that restrict who and what can reach in-scope systems?
- [ ] Are boundaries in place to protect in-scope systems from outside threats?
- [ ] Can you show these controls worked throughout the audit period, not just on one day?

Every framework

The questions almost every auditor asks

- [ ] Is your network diagram up to date?
- [ ] Can you show what changed since your last audit?
- [ ] Can you prove segmentation works as designed today, not just on the day it was tested?

Proving it once a year is hard. Proving it every day is harder.

Tufin Segmentation Intelligence keeps checking that your network is still divided the way you intended, flags where it has slipped, and keeps proof ready for your next audit.

See how it works →

General guidance only, not legal or audit advice. Requirements vary by framework version and assessor, so confirm scope with your auditor. The HIPAA Security Rule update is proposed and not yet final. Framework references current as of October 2026.