Compliance Mapping Methodology

TurboPentest · Mapping version 2026.08.12 · Generated 2026-10-31

This document explains how TurboPentest maps discovered cloud resources to compliance controls. It is the authoritative reference cited in every compliance evidence package generated by TurboPentest.

Principles

- Mappings are resource-type driven - every resource of a given type pulls the same controls.
- Only controls that pentesting can provide evidence for are included. Policy, HR, and physical controls are deliberately excluded.
- PCI-DSS v4.0 Req 11.4.3 (external) vs 11.4.2 (internal) routing - formerly Req 11.3.1 / 11.3.2 under v3.2.1 - is based on exposure tier (public / edge / at-risk ’ 11.4.3 external, private ’ 11.4.2 internal).
- Scope overrides are per-user and logged as events.
- A verified domain with a completed external pentest additionally evidences the vulnerability-management controls a black-box external test supports (SOC 2 CC7.1, ISO 27001 A.8.8, HIPAA 164.308(a)(1)). An untested domain maps only to PCI-DSS 11.4.3 external scope. Web-app and secure-coding controls (SOC 2 CC6.1, PCI 6.2.4, ISO A.8.26 / A.8.28 / A.8.29) are excluded from a domain pentest and are evidenced only by connected-repo source analysis.
- Secure-coding controls (PCI DSS 6.2.4, ISO 27001 A.8.28 / A.8.29) attest to practice in source code and are credited to an asset only when white-box source-analysis evidence exists; a black-box pentest alone does not evidence them.
- Only technical safeguards a test can evidence are mapped. HIPAA physical safeguards (e.g. 164.310 Facility Access Controls) are excluded from every technical mapping.
- PCI DSS v4.0 Req 6.4.1 (public-facing web applications reviewed for vulnerabilities) is evidenced by our external pentest for public-facing web apps and tested domains. Req 6.4.2 (automated technical solution / WAF) is not claimed - we detect a WAF but are not one, so WAF detection is reported only as an observation.

> **PCI DSS v4.0 11.4.5 scope note**
> TurboPentest tests from the internet today (external pentest scope, Req 11.4.3). PCI-DSS Requirement 11.4.5 internal segmentation testing requires testing inside your network - coming soon via our on-premises agent. For PCI Req 11.4.5 today, pair TurboPentest's external pentest with a traditional internal pentest from a qualified firm.

Resource type ’ controls

RESOURCE	EXPOSURE	CONTROLS
alb	public	SOC 2: CC6.6, HIPAA: 164.312(e)(1), ISO 27001: A.8.20, ISO 27001: A.8.24, PCI-DSS: 11.4.3
nlb	public	SOC 2: CC6.6, HIPAA: 164.312(e)(1), ISO 27001: A.8.20, ISO 27001: A.8.24, PCI-DSS: 11.4.3
load-balancer	public	SOC 2: CC6.6, HIPAA: 164.312(e)(1), ISO 27001: A.8.20, ISO 27001: A.8.24, PCI-DSS: 11.4.3
http-load-balancer	public	SOC 2: CC6.6, HIPAA: 164.312(e)(1), ISO 27001: A.8.20, ISO 27001: A.8.24, PCI-DSS: 11.4.3
load_balancer	public	SOC 2: CC6.6, HIPAA: 164.312(e)(1), ISO 27001: A.8.20, ISO 27001: A.8.24, PCI-DSS: 11.4.3
cloudfront-distribution	public	SOC 2: CC6.6, HIPAA: 164.312(e)(1), ISO 27001: A.8.20, ISO 27001: A.8.24, PCI-DSS: 11.4.3
front-door	public	SOC 2: CC6.6, HIPAA: 164.312(e)(1), ISO 27001: A.8.20, ISO 27001: A.8.24, PCI-DSS: 11.4.3

api-gateway	public	SOC 2: CC6.1, SOC 2: CC7.1, PCI-DSS: 6.2.4, HIPAA: 164.312(a)(1), HIPAA: 164.308(a)(1), ISO 27001: A.8.8, ISO 27001: A.8.26, ISO 27001: A.8.28, ISO 27001: A.8.29, PCI-DSS: 11.4.3, PCI-DSS: 6.4.1
api-management	public	SOC 2: CC6.1, SOC 2: CC7.1, PCI-DSS: 6.2.4, HIPAA: 164.312(a)(1), HIPAA: 164.308(a)(1), ISO 27001: A.8.8, ISO 27001: A.8.26, ISO 27001: A.8.28, ISO 27001: A.8.29, PCI-DSS: 11.4.3, PCI-DSS: 6.4.1
appsync-api	public	SOC 2: CC6.1, SOC 2: CC7.1, PCI-DSS: 6.2.4, HIPAA: 164.312(a)(1), HIPAA: 164.308(a)(1), ISO 27001: A.8.8, ISO 27001: A.8.26, ISO 27001: A.8.28, ISO 27001: A.8.29, PCI-DSS: 11.4.3, PCI-DSS: 6.4.1
app	public	SOC 2: CC6.1, SOC 2: CC7.1, PCI-DSS: 6.2.4, HIPAA: 164.312(a)(1), HIPAA: 164.308(a)(1), ISO 27001: A.8.8, ISO 27001: A.8.26, ISO 27001: A.8.28, ISO 27001: A.8.29, PCI-DSS: 11.4.3, PCI-DSS: 6.4.1
app-service	public	SOC 2: CC6.1, SOC 2: CC7.1, PCI-DSS: 6.2.4, HIPAA: 164.312(a)(1), HIPAA: 164.308(a)(1), ISO 27001: A.8.8, ISO 27001: A.8.26, ISO 27001: A.8.28, ISO 27001: A.8.29, PCI-DSS: 11.4.3, PCI-DSS: 6.4.1
cloud-run	public	SOC 2: CC6.1, SOC 2: CC7.1, PCI-DSS: 6.2.4, HIPAA: 164.312(a)(1), HIPAA: 164.308(a)(1), ISO 27001: A.8.8, ISO 27001: A.8.26, ISO 27001: A.8.28, ISO 27001: A.8.29, PCI-DSS: 11.4.3, PCI-DSS: 6.4.1
app-engine	public	SOC 2: CC6.1, SOC 2: CC7.1, PCI-DSS: 6.2.4, HIPAA: 164.312(a)(1), HIPAA: 164.308(a)(1), ISO 27001: A.8.8, ISO 27001: A.8.26, ISO 27001: A.8.28, ISO 27001: A.8.29, PCI-DSS: 11.4.3, PCI-DSS: 6.4.1
elastic-beanstalk	public	SOC 2: CC6.1, SOC 2: CC7.1, PCI-DSS: 6.2.4, HIPAA: 164.312(a)(1), HIPAA: 164.308(a)(1), ISO 27001: A.8.8, ISO 27001: A.8.26, ISO 27001: A.8.28, ISO 27001: A.8.29, PCI-DSS: 11.4.3, PCI-DSS: 6.4.1
vercel-project	public	SOC 2: CC6.1, SOC 2: CC7.1, PCI-DSS: 6.2.4, HIPAA: 164.312(a)(1), HIPAA: 164.308(a)(1), ISO 27001: A.8.8, ISO 27001: A.8.26, ISO 27001: A.8.28, ISO 27001: A.8.29, PCI-DSS: 11.4.3, PCI-DSS: 6.4.1
netlify-site	public	SOC 2: CC6.1, SOC 2: CC7.1, PCI-DSS: 6.2.4, HIPAA: 164.312(a)(1), HIPAA: 164.308(a)(1), ISO 27001: A.8.8, ISO 27001: A.8.26, ISO 27001: A.8.28, ISO 27001: A.8.29, PCI-DSS: 11.4.3, PCI-DSS: 6.4.1
replit-app	public	SOC 2: CC6.1, SOC 2: CC7.1, PCI-DSS: 6.2.4, HIPAA: 164.312(a)(1), HIPAA: 164.308(a)(1), ISO 27001: A.8.8, ISO 27001: A.8.26, ISO 27001: A.8.28, ISO 27001: A.8.29, PCI-DSS: 11.4.3, PCI-DSS: 6.4.1
spaces_cdn	public	SOC 2: CC6.6, HIPAA: 164.312(e)(1), ISO 27001: A.8.20, ISO 27001: A.8.24, PCI-DSS: 11.4.3
rds-instance	private	SOC 2: CC6.1, SOC 2: CC7.1, PCI-DSS: 6.2.4, HIPAA: 164.312(a)(1), HIPAA: 164.312(e)(1), ISO 27001: A.5.15, ISO 27001: A.8.3, ISO 27001: A.8.8, ISO 27001: A.8.24, PCI-DSS: 11.4.2
ec2-instance	private	SOC 2: CC6.1, SOC 2: CC6.6, PCI-DSS: 2.2, HIPAA: 164.312(a)(1), ISO 27001: A.8.8, ISO 27001: A.8.9, ISO 27001: A.8.29, PCI-DSS: 11.4.2
virtual-machine	private	SOC 2: CC6.1, SOC 2: CC6.6, PCI-DSS: 2.2, HIPAA: 164.312(a)(1), ISO 27001: A.8.8, ISO 27001: A.8.9, ISO 27001: A.8.29, PCI-DSS: 11.4.2
compute-instance	private	SOC 2: CC6.1, SOC 2: CC6.6, PCI-DSS: 2.2, HIPAA: 164.312(a)(1), ISO 27001: A.8.8, ISO 27001: A.8.9, ISO 27001: A.8.29, PCI-DSS: 11.4.2
lightsail-instance	private	SOC 2: CC6.1, SOC 2: CC6.6, PCI-DSS: 2.2, HIPAA: 164.312(a)(1), ISO 27001: A.8.8, ISO 27001: A.8.9, ISO 27001: A.8.29, PCI-DSS: 11.4.2
droplet	private	SOC 2: CC6.1, SOC 2: CC6.6, PCI-DSS: 2.2, HIPAA: 164.312(a)(1), ISO 27001: A.8.8, ISO 27001: A.8.9, ISO 27001: A.8.29, PCI-DSS: 11.4.2
lambda-function	private	SOC 2: CC6.1, SOC 2: CC7.1, PCI-DSS: 6.2.4, HIPAA: 164.312(a)(1), HIPAA: 164.312(e)(1), ISO 27001: A.8.8, ISO 27001: A.8.28, ISO 27001: A.8.29, PCI-DSS: 11.4.2
function-app	private	SOC 2: CC6.1, SOC 2: CC7.1, PCI-DSS: 6.2.4, HIPAA: 164.312(a)(1), HIPAA: 164.312(e)(1), ISO 27001: A.8.8, ISO 27001: A.8.28, ISO 27001: A.8.29, PCI-DSS: 11.4.2
cloud-function	private	SOC 2: CC6.1, SOC 2: CC7.1, PCI-DSS: 6.2.4, HIPAA: 164.312(a)(1), HIPAA: 164.312(e)(1), ISO 27001: A.8.8, ISO 27001: A.8.28, ISO 27001: A.8.29, PCI-DSS: 11.4.2

ecs-service	private	SOC 2: CC6.1, SOC 2: CC7.1, PCI-DSS: 6.2.4, HIPAA: 164.312(a)(1), HIPAA: 164.308(a)(1), ISO 27001: A.8.8, ISO 27001: A.8.26, ISO 27001: A.8.28, ISO 27001: A.8.29, PCI-DSS: 11.4.2
opensearch-domain	private	SOC 2: CC6.1, SOC 2: CC7.1, PCI-DSS: 6.2.4, HIPAA: 164.312(a)(1), HIPAA: 164.312(e)(1), ISO 27001: A.5.15, ISO 27001: A.8.3, ISO 27001: A.8.8, ISO 27001: A.8.24, PCI-DSS: 11.4.2
aks-cluster	private	SOC 2: CC6.1, SOC 2: CC6.6, PCI-DSS: 2.2, HIPAA: 164.312(a)(1), ISO 27001: A.8.8, ISO 27001: A.8.9, ISO 27001: A.8.29, PCI-DSS: 11.4.2
gke-cluster	private	SOC 2: CC6.1, SOC 2: CC6.6, PCI-DSS: 2.2, HIPAA: 164.312(a)(1), ISO 27001: A.8.8, ISO 27001: A.8.9, ISO 27001: A.8.29, PCI-DSS: 11.4.2
static-web-app	edge	SOC 2: CC6.6, HIPAA: 164.312(e)(1), ISO 27001: A.8.20, ISO 27001: A.8.24, PCI-DSS: 11.4.3
route53-zone	edge	PCI-DSS: 11.4.3
dns-zone	edge	PCI-DSS: 11.4.3
cloud-dns-zone	edge	PCI-DSS: 11.4.3
domain	edge	PCI-DSS: 11.4.3
dns-subdomain	edge	PCI-DSS: 11.4.3

Changelog

v2026.08.12 - 2026-07: A verified domain with a completed external pentest now evidences SOC 2 CC7.1, ISO 27001 A.8.8, and HIPAA 164.308(a)(1) in addition to PCI-DSS 11.4.3; untested domains remain PCI-scope only. 2026-05: Updated PCI DSS references to v4.0 numbering - Req 11.4 replaces v3.2.1 Req 11.3 sitewide (11.4.3 external / 11.4.2 internal / 11.4.5 segmentation). 2026-04: Added PCI DSS Req 11.4.5 internal-segmentation scope note; compliance mapping PDF download added. Initial published mapping; added ISO 27001, fixed PCI external/internal routing, added at-risk exposure tier routing.