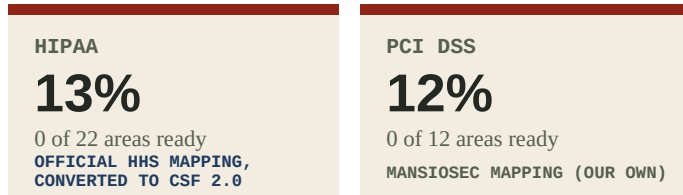


EXAMPLE SECURITY PARTNERS

AUDIT READINESS

Sample Dental Group (made up)

As of Oct 16, 2026 · From the NIST CSF 2.0 assessment loaded Oct 16, 2026 · Level expected: 3



The percentage is the share of linked CSF outcomes scored at level 3 or above. An area is Ready at 85% or more, Close at 50% or more, and Far below that.

This is an estimate for planning, not an audit opinion. Each framework below names where its mapping comes from. NIST SP 800-53 and SP 800-171 use NIST's official informative references, linked at subcategory level; they show which controls relate to a CSF outcome, not that a control is in place. HIPAA uses the official HHS Office for Civil Rights crosswalk to the NIST CSF (2016), converted to CSF 2.0 with NIST's references; HHS says it is an informative reference that does not imply or guarantee compliance. SOC 2, ISO 27001 and PCI DSS use MansioSec's own category-level mapping, not an official crosswalk. An auditor tests specific controls and evidence that a CSF score does not cover.

Source: HHS Office for Civil Rights, HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework (February 2016), converted to CSF 2.0 with the NIST CSF 2.0 Reference Tool's CSF v1.1 references. Neither HHS nor NIST endorses MansioSec.

HIPAA SECURITY RULE (45 CFR PART 164, SUBPART C)

Mapping: Official mapping: HHS OCR crosswalk (2016), converted to CSF 2.0 with NIST's references (CSF 1.0 to 2.0 through the NIST CSF 2.0 Reference Tool's CSF v1.1 lineage), subcategory level, HHS crosswalk February 2016, NIST data generated Oct 19, 2026.

This covers the Security Rule only. The Privacy Rule and Breach Notification Rule have their own requirements that the CSF does not measure. Each area is one of the Security Rule's 22 standards. HHS mapped every safeguard to at least one CSF subcategory but says the crosswalk cannot be relied on entirely for compliance; Security Rule requirements for documentation and organization map only in part. DE.DP-2 in the crosswalk has no CSF 2.0 subcategory successor, so it is not counted.

Ref	Area	Status	At level 3+	Average	Lowest outcomes
164.308(a)(1)	Security Management Process	Far	7 of 39	1.7	DE.AE-07 (0), GV.RM-02 (0), DE.AE-03 (1), DE.CM-01 (1), DE.CM-03 (1) +27 more
164.308(a)(2)	Assigned Security Responsibility	Far	1 of 5	2.0	PR.AT-02 (1), GV.OC-02 (2), GV.RR-02 (2), GV.SC-02 (2)
164.308(a)(3)	Workforce Security	Far	4 of 17	2.0	DE.CM-03 (1), ID.AM-03 (1), ID.RA-03 (1), PR.AT-02 (1), GV.OC-02 (2) +8 more
164.308(a)(4)	Information Access Management	Far	2 of 15	2.0	ID.RA-03 (1), PR.IR-01 (1), GV.OC-01 (2), GV.OC-02 (2), GV.OC-05 (2) +8 more
164.308(a)(5)	Security Awareness and Training	Far	2 of 14	1.2	DE.AE-07 (0), DE.AE-03 (1), DE.CM-01 (1), DE.CM-03 (1), DE.CM-06 (1) +7 more

Ref	Area	Status	At level 3+	Average	Lowest outcomes
164.308(a)(6)	Security Incident Procedures	Far	1 of 25	1.1	DE.AE-07 (0), GV.RM-02 (0), DE.AE-02 (1), DE.AE-03 (1), DE.AE-04 (1) +19 more
164.308(a)(7)	Contingency Plan	Far	3 of 25	1.5	GV.RM-02 (0), ID.IM-02 (0), GV.OC-04 (1), ID.AM-05 (1), ID.IM-03 (1) +17 more
164.308(a)(8)	Evaluation	Far	0 of 13	1.3	DE.AE-07 (0), DE.AE-03 (1), DE.CM-01 (1), GV.OC-04 (1), ID.AM-03 (1) +8 more
164.308(b)(1)	Business Associate Contracts and Other Arrangements	Far	3 of 13	1.9	GV.RM-03 (1), GV.RM-04 (1), PR.AT-02 (1), PR.IR-01 (1), GV.OC-02 (2) +5 more
164.310(a)	Facility Access Controls	Far	4 of 29	1.6	GV.RM-02 (0), DE.CM-01 (1), DE.CM-03 (1), DE.CM-06 (1), GV.OC-04 (1) +20 more
164.310(b)	Workstation Use	Far	4 of 12	2.0	DE.CM-01 (1), DE.CM-03 (1), DE.CM-06 (1), PR.IR-01 (1), PR.AA-03 (2) +3 more
164.310(c)	Workstation Security	Far	4 of 9	2.1	DE.CM-01 (1), DE.CM-03 (1), DE.CM-06 (1), PR.DS-10 (2), PR.PS-01 (2)
164.310(d)	Device and Media Controls	Far	5 of 17	1.8	DE.AE-07 (0), DE.AE-03 (1), DE.CM-01 (1), DE.CM-03 (1), DE.CM-06 (1) +7 more
164.312(a)	Access Control	Far	5 of 21	1.9	DE.CM-03 (1), GV.OC-04 (1), ID.IM-04 (1), ID.RA-03 (1), PR.IR-01 (1) +11 more
164.312(b)	Audit Controls	Far	4 of 15	1.6	DE.AE-07 (0), DE.AE-03 (1), DE.CM-01 (1), DE.CM-03 (1), DE.CM-06 (1) +6 more
164.312(c)	Integrity	Close	2 of 4	2.0	ID.RA-03 (1), PR.IR-01 (1)
164.312(d)	Person or Entity Authentication	Far	2 of 6	2.2	DE.CM-03 (1), ID.AM-08 (2), PR.AA-01 (2), PR.AA-05 (2)
164.312(e)(1)	Transmission Security	Far	5 of 13	2.1	DE.CM-01 (1), DE.CM-03 (1), ID.RA-03 (1), PR.IR-01 (1), ID.AM-08 (2) +3 more
164.314(a)	Business Associate Contracts or Other Arrangements	Far	1 of 13	1.3	DE.AE-07 (0), DE.AE-03 (1), GV.OC-04 (1), ID.RA-06 (1), PR.AT-02 (1) +7 more
164.314(b)	Requirements for Group Health Plans	Far	3 of 9	1.8	DE.CM-01 (1), DE.CM-03 (1), DE.CM-06 (1), GV.OC-04 (1), ID.RA-06 (1) +1 more
164.316(a)	Policies and Procedures	Far	0 of 2	2.0	ID.RA-04 (2), ID.RA-05 (2)
164.316(b)	Documentation	Far	0 of 5	1.6	ID.IM-03 (1), ID.IM-04 (1), ID.AM-04 (2), ID.RA-01 (2), PR.IR-02 (2)

PCI DSS V4.0

Mapping: MansioSec mapping (our own), category level. Official source: PCI SSC: Mapping PCI DSS v4.0.1 to the NIST Cybersecurity Framework 2.0 (<https://blog.pcisecuritystandards.org/mapping-pci-dss-v4.0.1-to-the-nist-cybersecurity-framework-2.0>).

PCI DSS is prescriptive: it sets specific technical requirements for the cardholder data environment that a CSF score cannot confirm. Reducing scope is usually the first step.

Ref	Area	Status	At level 3+	Average	Lowest outcomes
Req 1	Network security controls	Far	0 of 4	1.5	PR.IR-01 (1), PR.IR-03 (1), PR.IR-02 (2), PR.IR-04 (2)
Req 2	Secure configurations	Far	1 of 5	2.0	PR.PS-04 (1), PR.PS-01 (2), PR.PS-03 (2), PR.PS-05 (2)
Req 3	Protect stored account data	Close	3 of 4	2.8	PR.DS-10 (2)
Req 4	Protect cardholder data in transit	Close	3 of 4	2.8	PR.DS-10 (2)
Req 5	Protect against malicious software	Far	2 of 10	1.8	DE.CM-01 (1), DE.CM-03 (1), DE.CM-06 (1), PR.PS-04 (1), DE.CM-02 (2) +3 more
Req 6	Secure systems and software	Far	1 of 15	1.5	ID.RA-08 (0), ID.RA-02 (1), ID.RA-03 (1), ID.RA-06 (1), ID.RA-07 (1) +9 more
Req 7	Restrict access by business need to know	Far	1 of 6	2.2	PR.AA-01 (2), PR.AA-02 (2), PR.AA-03 (2), PR.AA-04 (2), PR.AA-05 (2)
Req 8	Identify users and authenticate access	Far	1 of 6	2.2	PR.AA-01 (2), PR.AA-02 (2), PR.AA-03 (2), PR.AA-04 (2), PR.AA-05 (2)
Req 9	Restrict physical access	Far	1 of 13	1.8	ID.AM-03 (1), ID.AM-05 (1), ID.AM-07 (1), ID.AM-01 (2), ID.AM-02 (2) +7 more
Req 10	Log and monitor all access	Far	2 of 16	1.5	DE.AE-07 (0), DE.AE-02 (1), DE.AE-03 (1), DE.AE-04 (1), DE.AE-08 (1) +9 more
Req 11	Test security regularly	Far	1 of 19	1.3	ID.IM-02 (0), ID.RA-08 (0), DE.CM-01 (1), DE.CM-03 (1), DE.CM-06 (1) +13 more
Req 12	Policies and programs	Far	4 of 30	1.4	GV.RM-02 (0), GV.RM-01 (1), GV.RM-03 (1), GV.RM-04 (1), GV.RM-05 (1) +21 more

EVIDENCE REQUESTS: EXAMPLE COMPLIANCE REVIEWERS (MADE UP)

8 open, 3 past due, 2 with the auditor, 2 accepted.

ID	Ref	Request	Owner	Due	Status	Document or location
E-01	HIPAA 164.308(a)(1)	Most recent security risk analysis and the risk management plan that follows it.	Practice administrator	Oct 9, 2026 (past due)	Returned for more	2025 HIPAA security risk analysis
E-02	HIPAA 164.308(a)(2)	Document naming the security official and their duties.	Practice administrator	Oct 9, 2026	Accepted	Information Security Policy v1.2
E-03	HIPAA 164.308(a)(5)	Security awareness training records for all workforce members, last 12 months.	Office manager	Oct 9, 2026	Accepted	2026 HIPAA and phishing training completion report
E-04	HIPAA 164.308(a)(3)-(4)	Access review for the practice-management system and Microsoft 365, with leavers in the last 12 months.	Practice administrator	Oct 14, 2026 (past due)	Collecting	IT provider exporting user lists
E-05	HIPAA 164.308(a)(6)	Incident response procedure and the record of any security incidents in the last 12 months.	Practice administrator	Oct 14, 2026 (past due)	Collecting	Incident Response Plan (draft)
E-06	HIPAA 164.308(a)(7)	Contingency plan, backup schedule and the most recent restore test.	IT provider	Oct 23, 2026	Submitted	Backup schedule and quarterly restore test log
E-07	HIPAA 164.308(b)	Business associate agreements for all vendors that create, receive or keep patient data.	Practice administrator	Oct 23, 2026	Submitted	Business associate agreements (9 vendors)
E-08	HIPAA 164.312(b)	Audit log settings and an example of log review for the PMS and Microsoft 365.	IT provider	Oct 30, 2026	Requested	
E-09	HIPAA 164.312(c), (e)	Device encryption report and email encryption settings.	IT provider	Oct 30, 2026	Requested	Device encryption compliance report (IT provider)
E-10	PCI DSS Req 12	Payment processor's attestation for the card terminals and the practice's self-assessment questionnaire.	Office manager	Nov 13, 2026	Requested	Processor's merchant portal