

HITRUST CSF v11.9

Executive Brief



HITRUST v11.9 at a Glance

An incremental but strategic release: AI, cryptography, and mapping currency

71

authoritative sources now integrated

1

new source added: OWASP Top 10 for Agentic Applications 2026

7

sources removed from the framework

44

e1 requirement statements (up from 43); i1 count holds at 182 (24 reworded)

Bottom line: v11.9.0 extends HITRUST assurance to agentic AI, adds post-quantum cryptography consideration, aligns to NIST SP 800-53 Rev. 5.2.0, and removes seven sources. Framework structure (14 control categories, 49 objectives, 156 specifications) is unchanged.

HITRUST Authoritative Sources

1	16 CFR 314	25	GovRAMP r5	49	NIST SP 800-171 R2
2	16 CFR 681	26	OCR Guidance for Unsecured PHI	50	NIST SP 800-171 R3
3	201 CMR 17.00	27	Health Industry Cybersecurity Practices (HICP 2023)	51	NIST SP 800-172
4	Abu Dhabi Healthcare Information and Cyber Security Standard (ADHICS)	28	45 CFR HIPAA.SR	52	NRS 603A
5	AICPA Trust Services Criteria (TSP) 100	29	45 CFR HIPAA.BN	53	NY OHIP Moderate-Plus Security Baseline v5.0
6	Australian Prudential Regulation Authority (APRA CPS 230)	30	45 CFR HIPAA.PR	54	10 NY DoH 405.46
7	ASD Strategies to Mitigate Cybersecurity Incidents	31	IRS Pub 1075 (2021)	55	OCR Audit Protocol (2016)
8	BSI C5	32	ISO/IEC 23894:2023	56	PHIPA
9	California Consumer Privacy Act § 1798	33	ISO/IEC 27001:2022	57	OWASP AI Exchange
10	CIS Controls v8	34	ISO/IEC 27002:2022	58	OWASP ML Top 10
11	CMS ARC-AMPE	35	ISO/IEC 29100:2024	59	OWASP ASI Top 10
12	CMS ARS 5.1	36	ISO/IEC 29151:2017	60	OWASP LLM v2025
13	COBIT 2019	37	ISO 31000:2018	61	OECD Privacy Framework
14	Commonwealth of Virginia SEC530	38	MITRE ATLAS	62	PCI DSS v4.0.1
15	SGP SCA 2018	39	NAIC 668	63	Singapore MAS
16	CMMC 2.0	40	UK CAF	64	Singapore PDPA
17	Digital Personal Data Protection Act (India), 2023 [DPDPA]	41	NIS2	65	SCIDSA 4655
18	Digital Operational Resilience Act (DORA)	42	23 NYCRR 500 Second Amendment	66	Texas Identity Theft Enforcement and Protection Act (TX 521)
19	FFIEC Cybersecurity Assessment Tool (CAT)	43	NHS England Data Security and Protection Toolkit v7 [DSPT]	67	Texas Medical Records Privacy Act
20	FISMA	44	NIST AI RMF 1.0	68	TXRAMP r5
21	21 CFR 11	45	NIST CSF 2.0	69	HHS Cybersecurity Performance Goals
22	FedRAMP r5	46	NIST IR 8374	70	UK AI Guide
23	FedRAMP KSI	47	NIST SP 800-53 R5.2.0	71	VA Directive 6500
24	EU GDPR	48	NIST SP 800-137		

Healthcare Based

AI Based

Authoritative Source Changes

Keeping mappings current; seven sources removed in v11.9.0

Added & Refreshed

NIST SP 800-53 Rev. 5.2.0

Mapping refreshed to match the current NIST control catalog

OWASP Top 10 for Agentic Applications 2026

New mapping plus a selectable compliance factor

HIPAA Privacy & Security Rules

Targeted mapping changes based on entity-type applicability analysis

AI Security Certification

New "Agentic AI" selectable factor

Removed

NIST SP 800-53 r4

Superseded by Rev. 5 (now at 5.2.0)

ISO/IEC 27799:2016

ISO/IEC 29100:2011

APEC Cross-Border Privacy Rules (CBPR)

Data Governance Framework

HITRUST De-ID Framework

The Joint Commission

e1, i1 and r2 at a Glance

HITRUST offers multiple assessment types an organization may pursue, based on its risk profile and the level of assurance stakeholders need.

e1 Essentials

44 requirement statements

- Foundational cybersecurity hygiene
- For small or lower-risk organizations and startups
- Valid for 1 year
- Provides entry-level assurance
- Stepping stone to i1 and r2 (work carries forward)
- **AI add-on: ai1 (score ≥ 83)**

i1 Implemented

182 requirement statements

Full i1

- Threat-adaptive, implemented security controls
- For mid-sized, moderate-risk organizations
- Valid for 1 year
- Provides moderate assurance
- **AI add-on: ai1 (score ≥ 83)**

Rapid i1 Recertification

- Accelerated option for the next i1 certification
- Requires an active i1 on CSF v11+ with no material control degradation
- Tests a sample of 60 scored statements plus prior CAP items; other scores roll forward
- Same i1 report and certification; valid for 1 year

r2 Risk-based

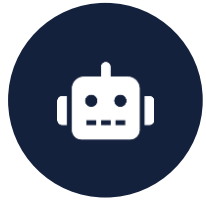
Tailored to your risk

- Comprehensive, risk-based assessment
- For large, regulated or high-risk organizations
- Requirements scoped by organizational, compliance and system factors
- Full maturity scoring: policy → managed
- Highest level of assurance
- Valid for 2 years (interim at year 1)
- **AI add-on: ai2 (score ≥ 62)**

Traversable: e1 ⊂ i1 ⊂ r2. Requirements at one level are included in the next, so earlier work is reused. Counts per CSF v11.9 baselines; v11.9 adds an "Agentic AI" factor to AI Security Certification.

CSF Library Enhancements

Control content updated for emerging technologies and risks



AI Security Certification

Content refined to support HITRUST's evolving AI assurance offerings.



AI Vulnerability Research

Requirements updated in response to AI-enabled vulnerability research.



PKI, TLS and Passkeys

Technology-specific requirements refreshed for modern authentication and encryption.

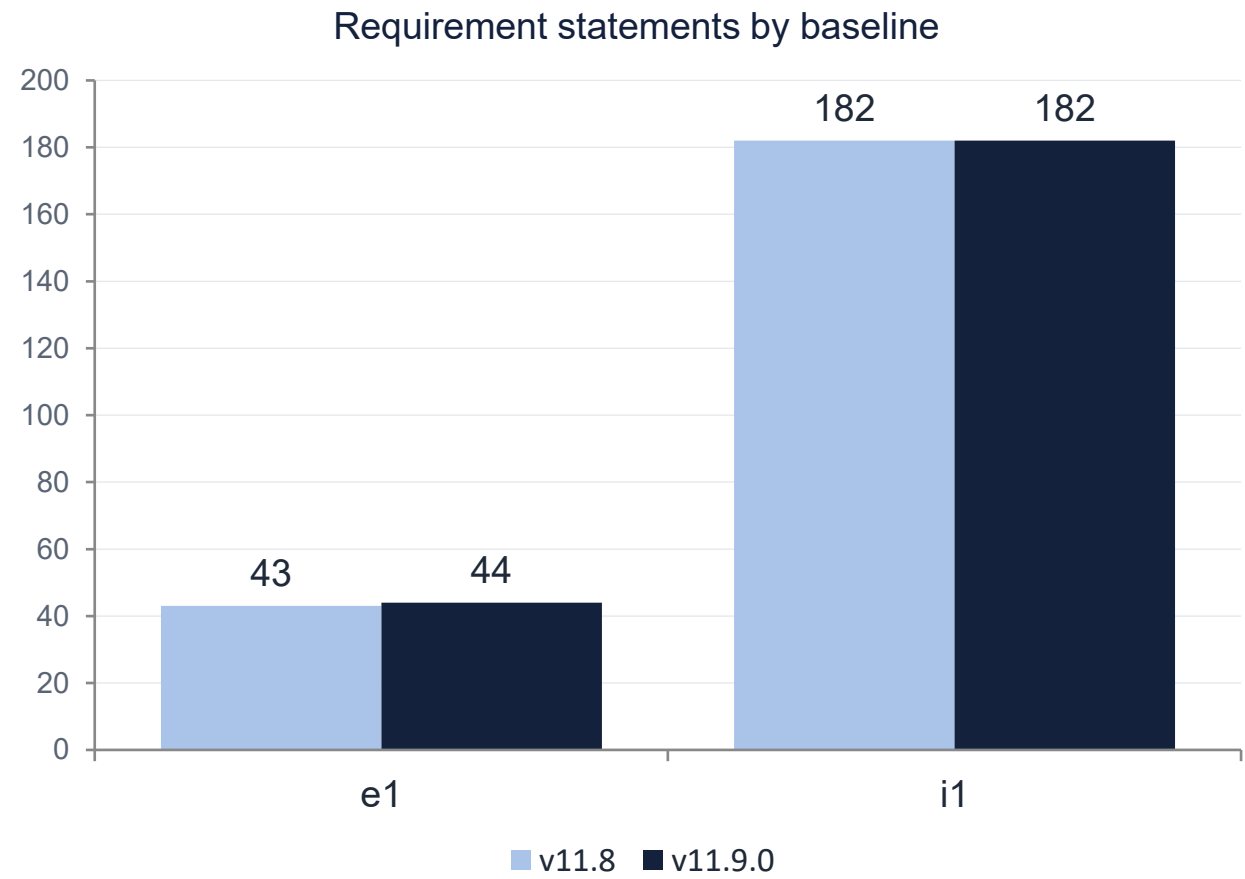


Post-quantum Cryptography

Documented quantum-resistance consideration added to e1 and i1 requirements.

Assessment Baseline Impact

Counts barely move, but requirement wording does; nesting across e1, i1 and r2 preserved



e1: +1 requirement

Baseline grows from 43 to 44 statements (one added, nine existing statements modified).



i1: Count unchanged

Baseline remains at 182 statements, but 24 statements were reworted.



Nesting preserved

All e1 requirements are in i1; all i1 requirements are in r2.

Rationale for the baseline change: see HITRUST's v11.9 Baseline Change FAQ.

AI is the Headline

v11.9.0 adds an explicit factor and mapping for agentic AI applications



Agentic AI factor

New selectable factor in the AI Security Certification for agentic applications.



OWASP Agentic Top 10

New mapping and compliance factor covering agent-specific risks such as tool misuse and goal manipulation.



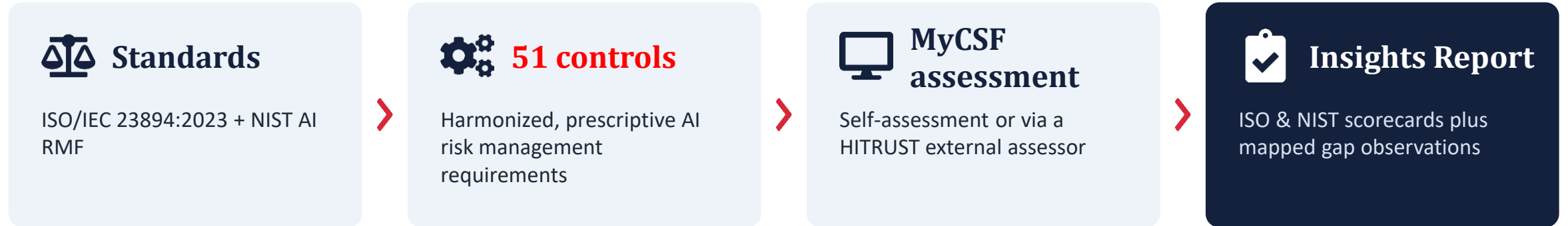
AI-enabled vuln research

Requirements updated in response to AI-enabled vulnerability research.

Builds on existing AI sources in the CSF: NIST AI RMF 1.0 · ISO/IEC 23894:2023 · MITRE ATLAS · OWASP LLM Top 10 (2025) · OWASP ML Top 10 · OWASP AI Exchange · UK Secure AI Guidelines

HITRUST AI Risk Management Assessment

A non-certified assessment of AI risk management maturity in ISO/IEC 23894 and NIST AI RMF terms



Harmonized controls

Built with industry working groups; 51 AI-specific controls inclusive of ISO/IEC 23894 and NIST AI RMF.

Management software

Runs on MyCSF; non-subscribers get one year of limited access to produce the report and scorecard.

Actionable reporting

Scores policy, process and implementation maturity and prioritizes gaps for remediation.

The bundle

- 1 AI Risk Management Insights Report
- 1 year of MyCSF SaaS access

Pricing on request from HITRUST

Existing HITRUST customers can add these controls to a current certification assessment for an assess-once effort.

HITRUST AI Security Assessment & Certification

Independent, certifiable proof that AI applications and platforms are secured



Comprehensive control set

Up to 44 AI-focused controls for AI platforms and systems.



Tailored control selection

Controls selected by AI deployment scenario and inherent risk (e.g., new Agentic AI factor in v11.9.0).



Rigorous assurance

Independent testing plus HITRUST centralized quality review.



Proactive threat adaptation

Quarterly control updates keep pace with AI threats.



Shared responsibility & inheritance

Inherit AI controls from HITRUST-certified cloud and service providers.

44

AI-focused controls (maximum)

~2 dozen

AI authoritative sources harmonized (NIST, ISO, OWASP and more)

99.62%

of HITRUST-certified environments reported no breaches in 2025

Choosing the Right AI Assessment

Insight into AI risk management vs. certified AI security

	AI Risk Management Assessment	AI Security Assessment & Certification
Primary question	Are we managing AI risk well?	Are our AI systems demonstrably secure?
Controls	51 AI risk management controls	Up to 44 AI security controls, tailored by risk
Basis	ISO/IEC 23894:2023, NIST AI RMF	NIST, ISO, OWASP and ~2 dozen AI sources
Assurance	Self-assessment or HITRUST external assessor	Independent testing + HITRUST QA review
Output	Insights Report & scorecard (not a certification)	HITRUST AI Security Certification (ai1/ai2, added to an e1, i1 or r2)
Best for	Organizations using or producing AI	AI application and platform providers

Who Values AI Certification

Security & risk teams

Sales & product leaders

TPRM programs

Boards & executives

Cyber insurers

Regulators

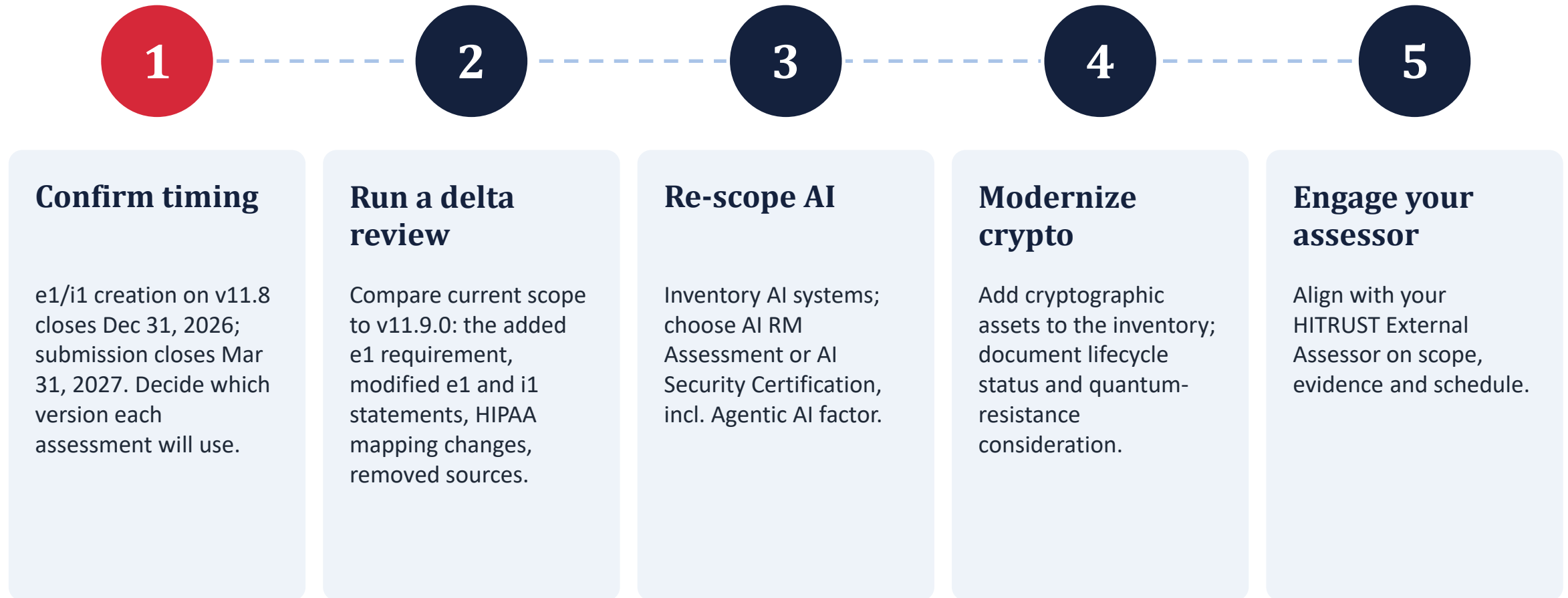
What it Means for Your Organization

Impact varies by assessment status and technology footprint

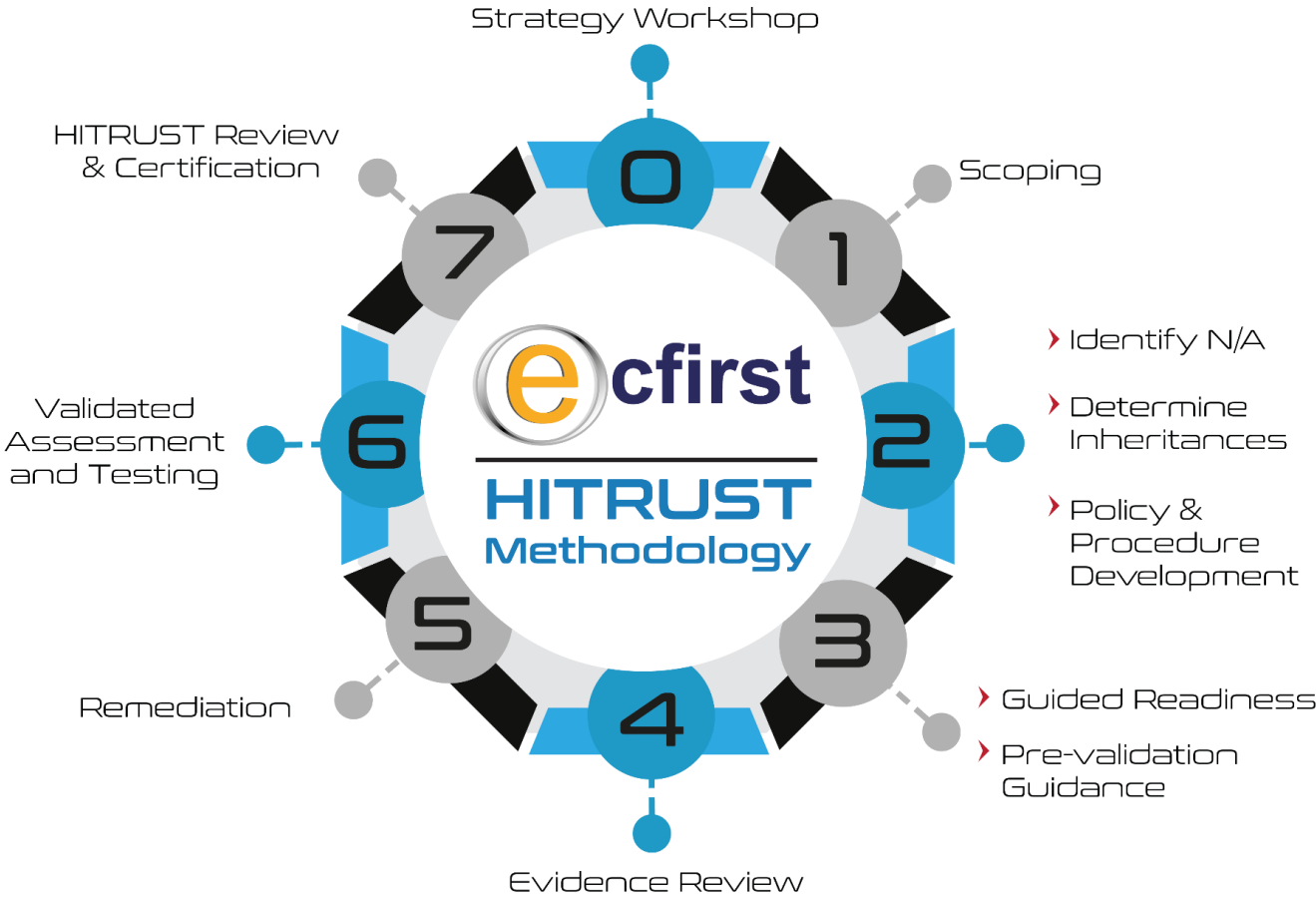
If you are...	What to consider	Impact
Currently assessing on v11.8	e1/i1 creation on v11.8 closes Dec 31, 2026; submission closes Mar 31, 2027 (HAA 2026-006). Plan the switch.	Medium
Deploying AI agents or LLM apps	Evaluate the Agentic AI factor and OWASP Agentic compliance factor for AI Security Certification.	High
HIPAA-covered entities & business associates	Review revised HIPAA Privacy/Security mappings against your entity type.	Medium
Relying on removed sources	Confirm reports that referenced NIST 800-53 r4, ISO 27799, etc. have replacement coverage.	Medium
All organizations	Inventory cryptographic assets, TLS and passkey use; document quantum-resistance consideration.	Medium
Running an r2 on v11.0 to v11.3	New r2 objects on those versions are disabled Dec 31, 2026; submission closes Mar 31, 2027 (HAA 2026-007).	Med–High

Recommended Next Steps

A practical path to v11.9.0 readiness



HITRUST & AI Methodology



Thank You!

@ Ali Pabrai | Ali.Pabrai@ecfirst.com

in <https://www.linkedin.com/in/pabrai/>



HITRUST
Authorized External Assessor

ecfirst