

HITRUST CSF

v11.9.0 | Facts

CSF v11.9.0 Updates

Newly Added Authoritative Sources

- ❖ OWASP Top 10 for Agentic Applications 2026 (a selectable Compliance factor, meaning organizations can choose to include it in scope).

Focus Areas Added: Agentic AI security, post-quantum cryptography, AI-enabled vulnerability research, and modern authentication and encryption.

Refreshed / Updated Sources & Mappings

- ❖ NIST SP 800-53 Rev. 5.2.0 mappings.
- ❖ HIPAA Privacy Rule and Security Rule mappings (based on which types of organizations each applies to).
- ❖ AI Security Certification content.

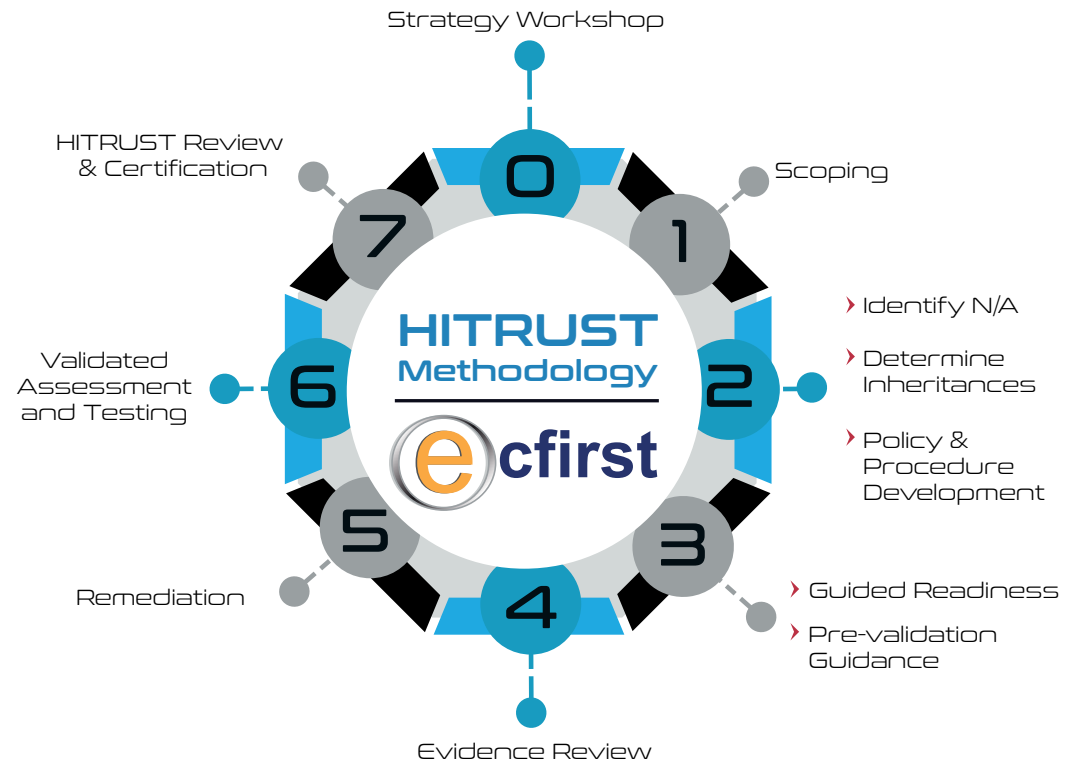
Removed Authoritative Sources

- ❖ APEC Cross-Border Privacy Rules (CBPR)
- ❖ Data Governance Framework
- ❖ HITRUST De-ID Framework
- ❖ ISO/IEC 27799:2016 and ISO/IEC 29100:2011
- ❖ NIST SP 800-53 Rev. 4
- ❖ The Joint Commission

Specific Requirement Changes

- ❖ New "Agentic AI" selectable factor in the AI Security Certification
- ❖ Refreshed technology requirements:
 - Public Key Infrastructure (PKI) and TLS
 - Passkeys and post-quantum cryptography considerations
- ❖ The e1 baseline grows to **44 requirements** (from 43); i1 stays at 182

ecfirst HITRUST Methodology



HITRUST CSF

v11.9.0 | Authoritative Sources

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

 New Additions

HITRUST CSF

v11.9.0 | Assessment Types

e1



(Essential - 1 Year)

i1



(Industry Best Practices - 1 Year)

r2



(Risk-Based - 2 Year)

Maturity Levels

Control Requirement Statements

Compliance Factors

Third Party Carve Outs

Certification Window

Supporting Assessments

Readiness	Validated
Implemented <i>Some testing requirements consider policy and procedure</i>	Implemented <i>Some testing requirements consider policy and procedure</i>
44	44
Yes - Limited (Insights Report)	Yes - Limited (Insights Report)
Yes	Yes
N/A	1 Year
N/A	Rapid (Qualifying Compliance Factors)

Readiness	Validated
Implemented <i>Some testing requirements consider policy and procedure</i>	Implemented <i>Some testing requirements consider policy and procedure</i>
182 <i>Core controls include e1 requirements</i>	182 <i>Core controls include e1 requirements</i>
Yes - Limited (Insights Report)	Yes - Limited (Insights Report)
Yes	Yes
N/A	1 Year
N/A	Rapid (Qualifying Compliance Factors)

Readiness	Validated
• Policy • Procedure • Implemented • Measured (Optional) • Managed (Optional)	• Policy • Procedure • Implemented • Measured (Optional) • Managed (Optional)
Risk Driven <i>Core controls include e1 and i1 requirements</i>	Risk Driven <i>Core controls include e1 and i1 requirements</i>
Yes - All Available	Yes - All Available
No	No
N/A	2 Years
N/A	• Interim • Bridge



Ali Pabani

Global AI Cyber Defense Thought Leader

HITRUST CSF

v11.9.0 | AI Assurance

AI Governance Bundle

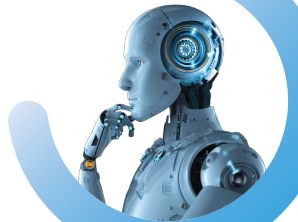


CAIO
Chief Artificial Intelligence Officer

AI Governance
On-Demand Consulting

AI Risk
Assessment
Report

ABC
CORP



ecfirst



aiCRP

AI Cyber Risk Professional

Online | Self-Paced

AI Certification
Training Program

HITRUST & AI Solutions

AI Risk Management Assessment

51
Controls

- ✦ Aligned with NIST AI RMF + ISO/IEC 23894:2023
- ✦ Identify gaps and prioritize actions
- ✦ Non-certified; focused on improving AI risk posture

AI Security Assessment & Certification

44
Requirements

- ✦ Formal HITRUST AI Security Certification
- ✦ Standalone or paired with HITRUST e1/i1/r2
- ✦ Designed for AI platforms, developers and deployers

AI Penetration Test



- Your AI Attack Surface
- Customized Approach
- Our Methodology
- Executive Dashboard

HITRUST
Authorized External Assessor

ecfirst

Ali Pabani

Global AI Cyber Defense Thought Leader