Deloitte.
Together makes progress

Hitrust
January 2026

Introduction: The evolving cybersecurity landscape

In today's hyper-connected and risk-charged environment, cybersecurity has shifted from an IT function to a **boardroom mandate**, driven by the rising scale and sophistication of cyberattacks, data breaches, and ransomware incidents. At the same time, organisations are managing unprecedented volumes of sensitive and AI-generated data—from PII and PHI to financial and operational information.

This convergence has led to **audit overload, escalating compliance costs, and growing organisational fatigue**. With credential-based attacks continuing to dominate breach activity, the need for a **unified, proactive, and certifiable security framework** that strengthens both protection and compliance has become increasingly clear.

Does your organisation face any of the below

- Managing ever-growing volumes of sensitive and AI generated data across cloud, on-premises, and hybrid environments
- Struggle to identify and address vulnerabilities and emerging threats in real time
- **Overlapping regulatory frameworks** (HIPAA, ISO 27001, NIST, PCI DSS, SOC 2, GDPR) driving audit duplication
- Growing third-party and vendor risk exposure
- Rising client and regulatory expectations for continuous, evidence-based assurance
- AI systems that require robust governance, security, and auditability

If your organisation faces these challenges, you're not alone.

Traditional, compliance-driven approaches are no longer enough to ensure security, trust, and efficiency. What's needed is a **unified, scalable, and certifiable framework** that brings together risk management, regulatory alignment, and continuous assurance.

This is where HITRUST comes in.

What is HITRUST?

HITRUST is a **comprehensive, certifiable, and scalable cybersecurity and compliance framework** that enables organisations to demonstrate trust, accountability, and consistent risk management. Originally focused on healthcare, it has become a **cross-industry benchmark** adopted across finance, technology, manufacturing, education, and the public sector.

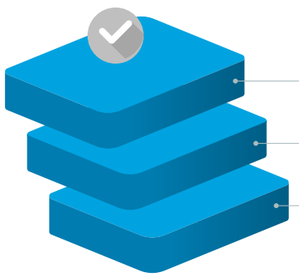
By **harmonising leading standards**—ISO 27001, NIST, HIPAA, PCI DSS, SOC 2, GDPR—into a **single, integrated, auditable framework**, HITRUST reduces complexity and elevates assurance.

HITRUST enables organisations to:

- Adopt a **consistent, risk-based approach** to security and privacy
- Replace multiple audits with **one unified assessment**
- Enhance organisational **resilience, transparency, and trust**
- Demonstrate **independently validated compliance** across stakeholders

In a world of decentralised data, unpredictable threats, and emerging AI risks, HITRUST provides a **trusted, measurable, and future-ready assurance model**.

HITRUST offers three levels of assurance:



Level	Purpose	Best for
e1 Foundational cybersecurity	Basic cybersecurity hygiene and essential controls	Small/mid-sized organisations starting a compliance journey
i1 Threat-adaptive assurance	Advanced, threat-based controls	Organisations managing sensitive data and third-party risks
r2 Comprehensive/customisable	Deep-dive certification	Enterprises requiring high assurance and multi-framework compliance

Each level builds on the previous, allowing organisations to scale without redoing prior work.

Why HITRUST?

HITRUST addresses modern security challenges—**fragmented regulations, cyber risk, AI governance, and supply chain exposure**—through a **single, risk-based assurance model** that scales with your organisation's needs.

Unified, rationalised framework
integrating ISO, NIST, HIPAA, GDPR, PCI DSS, and SOC 2 - eliminating audit overlap and ensuring consistent protection across cloud, on-premises, and hybrid environments.

Risk-based, data-centric controls
that strengthen safeguards for high-sensitivity and high-volume data.

Scalable assurance (e1, i1, r2)
aligned to organisational complexity and regulatory expectations.

Continuous monitoring and near real-time threat response
for faster detection and remediation.

Key capabilities

Key strengths include

AI and emerging tech assurance
aligned to NIST AI RMF and ISO/IEC 23894 for model integrity and accountability.

Enhanced third-party and supply-chain visibility
to reduce downstream risk.

Independent, globally recognised certification
that strengthens trust with clients and regulators.

Operational efficiency
by replacing multiple audits with one streamlined, proactive framework.

Value delivered

1. **Reduced audit overhead:** One evidence set satisfies multiple regulations, cutting audit spend and staff effort
2. **Lower breach risk:** Unified controls and continuous monitoring shrink the attack surface, as reflected by the near-zero breach rate among certified entities
3. **Accelerated time-to-market:** Faster, single-track certification enables quicker contract wins, especially in regulated supply chains
4. **Enhanced trust:** A globally recognised certification signals to customers, regulators and partners that security is "built-in"
5. **Future-proof governance:** Built-in AI risk controls keep organisations compliant as new technologies emerge
6. **Operational efficiency:** Fewer corrective action plans (up to 54% reduction for repeat i1 customers) translate into lower remediation costs and smoother security operations
7. **Lower audit costs and faster cycles:** Reusing evidence across multiple regimes cuts audit spend and shortens the time-to-certification, freeing resources for core business activities
8. **Trusted third-party certification:** Independent verification delivers a globally recognised "trusted" seal, restoring confidence among customers, partners and regulators

Why Deloitte?

Deloitte combines deep industry knowledge, a global delivery network, a suite of HITRUST specific services, and advanced AI risk governance, delivering a faster, smoother, and more streamlined assessment journey towards Hitrust certification than traditional consulting firms or boutique assessors that focus only on the audit itself. Choosing Deloitte means working with a team that not only assists you in getting HITRUST certified but also assists in embedding the aspects into your ongoing operations, supply chain, and emerging technology initiatives.

Our methodology

Readiness and gap assessment:
Review of your current security posture, benchmark it against the HITRUST framework, identify gaps with remediation action.

Remediation Implementation Support:
Assist the management in defining the required policies, procedures, and technical controls, to align them to remediate the identified gaps

Validated assessment and certification assistance:
As external assessors, we conduct control testing, validate evidence and document workpapers for submitting within MyCSF, and liaise with HITRUST throughout the review process to help ensure a smooth and timely certification from HITRUST.

AI control readiness:
Assist the organizations in preparing AI security and AI risk management controls aligned with HITRUST's AI standards ensuring readiness with governance framework, securing AI models and data while meeting emerging regulatory expectations

Contact Us

Anthony Crasto
Partner
acrasto@deloitte.com

Peeyush Vaish
Partner
peeyushvaish@deloitte.com

Karthik Ramachandran
Partner
rkaarthik@deloitte.com

Acknowledgement

Kedar Sawale
SME
ksawale@DELOITTE.com