HITRUST®

TRUST REPORT
2026

TACKLING THE TRUST CRISIS

Table of Contents

Message from HITRUST

This 2026 Annual Trust Report marks an important milestone. It is our third edition, now spanning four years of performance data across HITRUST-certified environments. Like HITRUST, the Trust Report has become the assurance industry gold standard, and the evidence is increasingly clear:

> *HITRUST represents the most reliable information risk assurance program available today and the only risk-based assurance system with statistically proven outcomes demonstrating breach rates reduced to a fraction of a percent.*

Perhaps more compelling: These results continue to improve year after year. Our reported breach-free performance has increased from 99.36% to 99.41%, and now to 99.62%. That progression is not accidental. It is the product of an assurance architecture designed for continuous evolution to serve today's information security programs.

HITRUST is built on two foundational pillars: relevance and reliability. Relevance through aligning with real-world threats and organizational demands. Reliability by providing assurance which includes accuracy, consistency, scalability, transparency, integrity, and efficiency.

These qualities are no longer optional. They are now crucial for the stakeholders making critical risk decisions every day — including Third-Party Risk Management (TPRM) leaders; cyber insurance underwriters; federal, state, and local governments; and increasingly boards of directors, private equity firms, and investors who are mandating defensible cyber risk governance. Today's enterprise information risk and cybersecurity leaders need more than compliance. They need to know what quantitatively and defensibly "good" looks like and the maturity of organizations against that standard.

HITRUST was built for this moment. We are seeing an increasingly large number of organizations interested in quantifying, reducing, and transferring their risk. These companies are coming to HITRUST to lower the cost and inefficiency of fragmented assurance, streamline third-party oversight, and create scalable trust across their supply chains.

Looking ahead, trust will be shaped by two defining forces: artificial intelligence and third-party dependency. AI introduces new categories of security risk that most assurance programs are not equipped to address. HITRUST is proud to lead the market with the only assurance program designed to evaluate the security of deployed AI systems, leveraging the same proven methodology that has driven measurable risk reduction for years.

We remain committed to continued investment in innovation to ensure HITRUST delivers early, maximum customer value and enduring confidence for every stakeholder depending on assurance.

Thank you to our customers, partners, assessors, employees, and stakeholders who continue building trust through HITRUST.

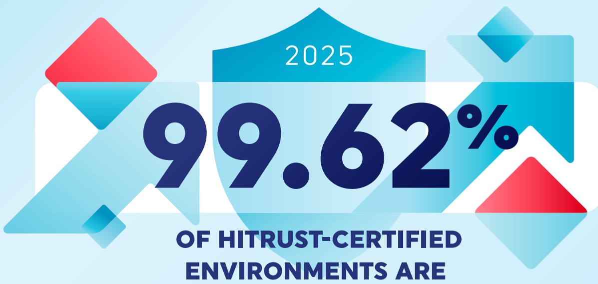
Sincerely,

Gregory Webb
Chief Executive Officer
HITRUST

TRUST REPORT 2026
AT A GLANCE

"47% of the interviewed companies had been affected by a cybersecurity breach."

— Munich RE's Global Cyber Risk and Insurance Survey 2024

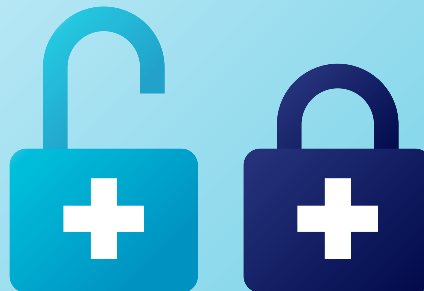


OF HITRUST-CERTIFIED ENVIRONMENTS ARE BREACH-FREE

While more than 40% of organizations report experiencing a breach, the breach rate for HITRUST-certified environments has continued a multi-year trend of exceptionally low breach rates.

"The average cost of a healthcare breach was $7.42M. The healthcare sector has been the costliest sector for a breach for 12 consecutive years."

— IBM's Cost of a Data Breach Report 2025



None of the top 50 healthcare breaches reported in the `Department of Health & Human Services OCR breach portal occurred in HITRUST-certified environments.

"CPAs warn that an ongoing push for high-volume SOC services may come at the cost of quality and objectivity"

— Journal of Accountancy | February 2026

THE MODERN ASSURANCE GAP

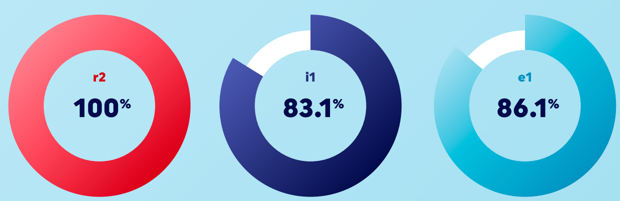
100%

of HITRUST certifications go through independent and centralized HITRUST Quality Review prior to issuance.

"...the percentages of breaches where a third party was involved doubled, going from 15% to 30%."

— 2025 Verizon Data Breach Investigations Report

HITRUST THIRD-PARTY COVERAGE



Over 80% of HITRUST certifications, including 100% of r2 certifications, addressed threats posed by the organization's service providers.

Executive Summary

Trust has emerged as a strategic asset in today's digital economy, but has become difficult to achieve. Organizations depend on complex, interconnected ecosystems of vendors, cloud platforms, and emerging technologies, while cyber threats continue to grow in scale, sophistication, and impact. These increasing cyber threats have caused third-party related breaches to *double* in just the last year[1].

Many assurance mechanisms are not keeping pace, creating a widening gap between the assurance which stakeholders *require* and the assurance those mechanisms are able to *deliver*. This inability for stakeholders to obtain relevant and reliable information security assurances is shaping a present-day Trust Crisis.

In the 2026 Trust Report we examine this Trust Crisis, analyzing the gaps causing this crisis, and demonstrating how HITRUST's evolving, threat-intelligent enabled assurance model addresses the shortcomings of traditional approaches.

2025

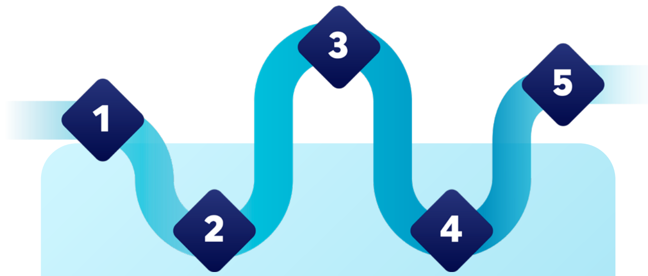
99.62%

OF HITRUST-CERTIFIED ENVIRONMENTS ARE BREACH-FREE

Breach Rates and the Trust Gap

There is a distinct contrast between the broader market and HITRUST-certified environments. In 2025, **99.62%** of HITRUST-certified environments did not report a breach in their certified environments, continuing a multi year trend of exceptionally low breach rates. In contrast, independent surveys allude to the fact that more than 40% of organizations have experienced a security breach[2].

While no centralized breach repository exists, this disparity between reported industry-wide breach rates and HITRUST-certified environments suggests that prescriptive, validated, and continuously updated assurance materially reduces the likelihood of a breach.

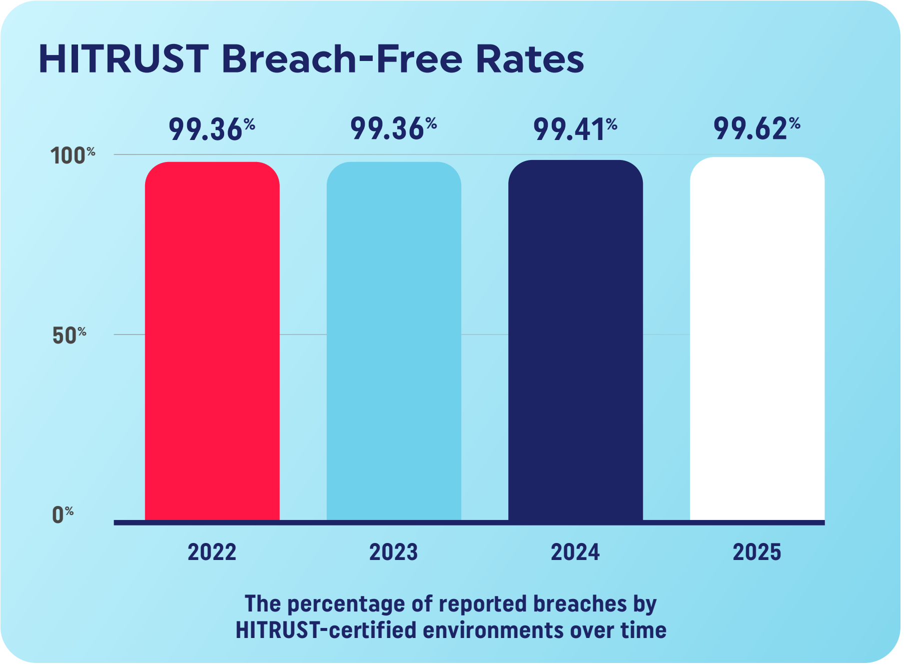


Stakeholder Roadmap to Success

Throughout this report, we have identified the various innovations HITRUST has introduced to bridge the present-day trust gap between organizations and their stakeholders. For stakeholders to be successful in managing their risk management programs, they should undertake the following:

1. **Shift from "flexible compliance" to threat-intelligent assurance:** Select assurance mechanisms that prescribe requirements aligned to real-world attack techniques.
2. **Verify assurance report integrity:** Find assurance providers who require independent and centralized quality reviews. This has the added benefit of reducing inconsistency and improving comparability across vendors.
3. **Reduce supply chain exposure:** Require assurance mechanisms which validate that organization's service providers rather than excluding them from scope.
4. **Secure AI before scale accelerates risk:** Require structured AI security assessments grounded in threat intelligence and governance controls.
5. **Reassess the definition of "good information security assurance":** Trust must be demonstrated through measurable outcomes and improvement, independent validation, and continuous adaptation to emerging threats.

The strength of the HITRUST program, which has allowed us to build Trust throughout the HITRUST community, is in the design of the framework and assurance process to promote *relevant* assurances. We have taken a unique approach to our framework design when compared to other legacy assurance providers.



Other assurance processes emphasize flexibility and principle-based guidance, placing significant responsibility (and burden) on organizations to define and justify their own controls. While this "flexible compliance" can reduce friction during assessments, it introduces inconsistent coverage, blind spots, and misaligned incentives, making them inappropriate for stakeholders attempting to evaluate the trustworthiness of its vendors.

Unlike legacy assurance frameworks, HITRUST provides explicit, prescriptive requirements designed to mitigate specific attack paths identified from its continuous stream of threat intelligence data. HITRUST's Cyber-Threat Adaptive (CTA) capability allows the framework to evolve based on objective intelligence rather than slow, consensus-driven updates. CTA ensures that our requirements evolve in direct response to the changing threat landscape, grounding security controls using real-world attack data. This reduces ambiguity for organizations while ensuring that certifications reflect genuinely relevant security outcomes rather than minimal compliance.

The HITRUST Advantage

HITRUST uses a centralized distribution model for all issued reports and certifications. This enables a level of data-driven insight which is not possible in decentralized programs. Since HITRUST manages the assessment process and report issuance through its platform, we can aggregate our data to produce this Trust Report.

In contrast, other legacy assurance platforms have no direct access to assessment results or ongoing performance data for their reports and/or certifications. The underlying assessments for most legacy assurance mechanisms do not go through quality procedures independent from the issuing firm prior to publication.

> Meanwhile, all HITRUST assessments are submitted to HITRUST for independent quality review and only issued by HITRUST.

Our centralized model provides deliberate and immediate feedback loops with the firms performing HITRUST assessments. This continuously improves the quality of subsequent assessments in real time; something that is not possible in decentralized assurance models.

The Need to Address Third-Party Risk

Vendor risk continues to grow through the proliferation of breaches originating within supply chains. In addition to the doubling of supply chain attacks[3], 54% of large organizations identified supply chain challenges as the biggest barrier to achieving cyber resilience[4].

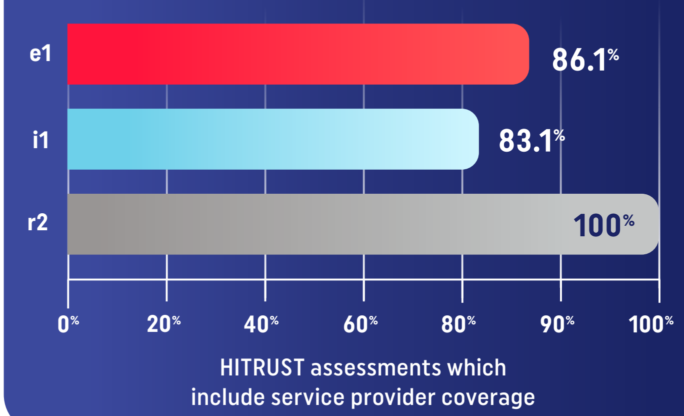
> To manage these risks, over 80% of HITRUST certifications, including 100% of r2 certifications, address the threats presented by an organization's service providers.

Comparatively, many legacy assurance providers do not require or have service provider coverage in any of their published assurance reports. The complexity involved with addressing risks across multiple third parties often creates this coverage limitation in other assurance provider assessments.

A unique innovation to efficiently address service provider risk in a HITRUST assessment is through our inheritance functionality. HITRUST's inheritance functionality allows organizations to reuse validated controls from cloud providers, vendors, and prior assessments through structured shared responsibility matrices.

In 2025, 69.7% of all HITRUST assessments used the inheritance functionality, an increase of 5.6% from 2024. No other major assurance provider offers a comparable inheritance mechanism, making this capability a critical differentiator in managing supply-chain risk without multiplying the assessment burden.

HITRUST Third-Party Coverage



HITRUST Inheritance Functionality

In addition to strengthening assurance, HITRUST's inheritance functionality improves assessment efficiency. When comparing HITRUST assessments using external inheritance to those that did not use inheritance:

On average, external assessors spent:

11.5% FEWER HOURS on all assessment types which used inheritance

19.4% FEWER HOURS on r2 assessments which used inheritance

34.8% FEWER HOURS on i1 assessments which used inheritance

Non-HITRUST Certified Healthcare Environments Continue to Struggle

Healthcare remains the most heavily impacted industry, reinforcing the urgency of trustworthy assurance.

- Healthcare was the most breached industry, accounting for nearly a quarter (23%) of breaches[5].
- The average cost of a healthcare cyber incident reached $7.42 million[6], reflecting both operational disruption and regulatory exposure.
- In HITRUST assessments, the healthcare sector continued to score lower on average than other industries, particularly when compared to the financial services sector.

Based upon HITRUST's review, **none of the top 50** healthcare breaches reported in the OCR breach portal in 2025 occurred in HITRUST-certified environments.

- Public data from the U.S. Department of Health and Human Services Office for Civil Rights (OCR) breach portal further highlights the challenge: 710 data breaches were published into the portal in 2025, impacting a total of 61,556,256 individuals[7].

Almost a quarter (24.5%) of HITRUST certifications are within the Healthcare sector. Our low breach rate reflects that those Healthcare companies who become HITRUST-certified can materially offset these sector-specific risks.

The Future of Trust

The Future of Trust needs assurance providers that can keep pace with rapidly evolving technologies, threat actors, and interconnected ecosystems. As organizations increasingly deploy AI and deepen reliance on complex third-party supply chains, traditional assurance mechanisms are proving to be insufficient. Trust can no longer be established through principle-based frameworks or self-defined controls that lag behind real-world threats. Instead, restoring confidence requires assurance that is prescriptive, threat-intelligent, independently validated, and continuously updated to reflect how modern attacks actually occur.

By aligning assurance with real-world threats and measurable outcomes, we believe it is possible not only to address today's Trust Crisis, but to build a more resilient and trustworthy digital future.

HITRUST is extending its threat-aligned assurance philosophy into two critical areas shaping the next era of risk: Artificial Intelligence and Third-Party Risk Management (TPRM). Through its AI Security Certification, HITRUST provides organizations with a structured, risk-based approach to securing deployed AI systems, translating emerging AI risks into concrete, implementable controls that build on established governance and security practices. Simultaneously, HITRUST's approach to TPRM delivers consistent, comparable, and decision-ready assurance across vendor ecosystems.

Trust today requires aligning assurance with real-world threats and measurable outcomes to build a more resilient and trustworthy digital future. HITRUST's assurance program is designed to meet that bar at scale.

THE TRUST CRISIS

Today's assurance providers have a responsibility to provide trustworthy assurance grounded in real-world threats, independent oversight, and measurable outcomes.

The Trust Crisis

Trust is built on the belief that the systems, technologies, and partners a company depends on will protect its data, act responsibly, and remain secure. Trust is a strategic asset that shapes how organizations communicate, collaborate, and create value together. When trust is present, teams and partners operate with greater transparency, confidence, and efficiency. When it is absent, initiatives can stall under the weight of doubt, misalignment, and unnecessary friction.

There is a growing sense that organizations can no longer confidently rely on the security of the systems, technologies, and partners they depend on. There are several reasons for this developing crisis in trust:

Rising supply chain attacks:

Vendors and service providers are increasingly being targeted, knowing that a compromise of one supplier can provide an attacker access to hundreds or thousands of downstream customers.

"For this year, we found third-party involvement of some sort in 30% of all breaches we analyzed, up from roughly 15% last year."

– Verizon 2025 Data Breach Investigations Report (DBIR)[8]

Overlapping digital ecosystems:

Companies are trying to maintain oversight of dozens (sometimes hundreds) of connected systems, from payroll to cloud storage to AI platforms. Each additional system expands the "attack surface," creating new pathways for breaches.

"Only 3% of organizations have full insight across their entire supply chain, leaving them vulnerable to hidden risks."

– Panorays' 2025 CISO Survey[9]

Limited visibility:

Many organizations have little insight into how their vendors secure data. They often rely on questionnaires or marketing claims, which don't always reflect real security performance.

"Of large organizations, 54% identified supply chain challenges as the biggest barrier to achieving cyber resilience. The increasing complexity of supply chains, coupled with a lack of visibility and oversight into the security levels of suppliers, has emerged as the leading cybersecurity risk for organizations."

– World Economic Forum's Global Cybersecurity Outlook 2025[10]

Erosion of public confidence:

Information security incidents, such as ransomware on hospitals, data leaks from tech giants, or exposed customer data from cloud providers, have become regular headlines. This has caused public concerns around whether companies have the capabilities to appropriately manage their information security programs.

Who can I trust?

This crisis in trust has resulted in the above simple but elusive question.

In order to deliver the answer, assurance providers must adapt to handle the challenges present in today's information security landscape.

In this 2026 edition of the Trust Report, we will describe the innovations HITRUST has made and continues to make in order to provide *relevant* assessments with *reliable* results, allowing companies to find partners they can trust.

Evolution of Assurance

The assurance frameworks, programs, and reports in use today are the product of decades of changing technology, business models, regulatory pressure, and threat activity. By examining how *assurance providers* developed in response to earlier risks, we can better recognize where legacy approaches no longer align with modern realities and why continuous adaptation is now critical to sustaining trust.

In the early days of computing from the 1970s to 1990s, assurance was almost nonexistent. Security was a technical afterthought, managed by system administrators and engineers who understood the machines but not risk or governance concepts.

By the 1990s, globalization, the internet, and corporate outsourcing made the old trust model impossible. Organizations needed evidence that partners and vendors were operating securely, and businesses needed common language to describe risk.

This era produced the first major assurance providers:

- ISACA's COBIT (Control Objectives for Information Technologies) gave executives and auditors a governance blueprint for IT.
- ISO's BS 7799 (later ISO 27001/27002) introduced a structured approach to information security management.
- AICPA's SAS 70 (later Service Organization Control [SOC] reporting) provided a way for service organizations, like data centers, to demonstrate controlled environments.

Assurance Providers

The term "*assurance providers*" is used throughout this report to group together those assurance frameworks and programs used to guide an organization's information security program.

Assurance Framework: Standards and control catalogs that say what good cybersecurity looks like and often how to manage it.

Assurance Program: A program which includes rules and criteria for issuing assurance reports and/or certifications. These reports and certifications are intended to reliably convey a company's performance against one or more frameworks.

Certain assurance providers may only provide an assurance framework (e.g., COBIT, NIST), while other assurance providers will also maintain an assurance program supporting the issuance of assurance reports (e.g., SOC 2, PCI AoC/RoC) and/or assurance certifications (e.g., HITRUST, ISO 27001).

As e-commerce expanded in the early 2000s, so did breaches at retailers, banks, and government agencies. As a result, specific standards emerged to provide measurable, auditable, and repeatable assurance:

In **2004**, the PCI DSS (Payment Card Industry Data Security Standard) v1.0 was published, setting strict rules for protecting credit card data.

In **2005**, the first version of ISO 27001 was launched, emphasizing risk assessment and risk treatment (but with more prescriptive guidance than later versions). ISO 27001 became the global language of security maturity, and organizations sought certification to demonstrate disciplined security management.

HITRUST was founded in **2007** to assist companies with addressing the growing regulatory pressure in the Healthcare industry, especially around HIPAA.

In March **2009**, HITRUST launched the CSF (Common Security Framework) as a unified, certifiable control framework to give organizations a structured, prescriptive, and auditable approach to protecting sensitive health/medical data.

In April **2010**, the AICPA launched SSAE 16 (Statement on Standards for Attestation Engagements No. 16), which superseded SAS 70 and laid the groundwork for a new suite of Service Organization Control (SOC) reports. SOC 2 was designed to address assurance around nonfinancial controls relevant for technology, cloud, and service organizations (i.e., not just financial-reporting firms).

The next wave of assurance in the 2010s brought a further shift in thinking about information security. Rather than simply protecting the environment, the concept of cyber resilience was introduced as a process for identifying and responding to breaches.

- NIST CSF (Cybersecurity Framework) was born from national-level concerns about critical infrastructure. It made assurance not just about preventing failures, but also about proving resilience

Throughout the previous decades since being launched, the HITRUST CSF expanded to incorporate a universe of relevant standards, best practices, and regulations from ISO, AICPA, NIST, and other authoritative sources to make a HITRUST certification suitable for organizations of all types and sizes, regardless of industry.

Authoritative Source

An authoritative source is a relevant standard, best practice framework, or regulation. Examples of authoritative sources included in the HITRUST CSF are:

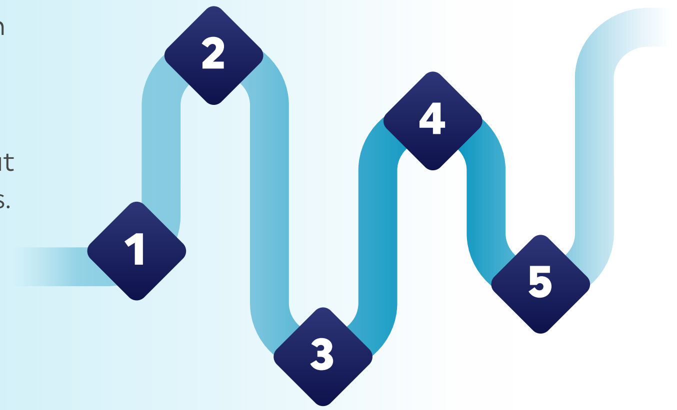
- NIST Cybersecurity Framework (CSF) v1.1 and 2.0
- NIST Special Publication 800-53 Revisions 4 and 5
- Center for Internet Security (CIS) Critical Security Controls (CSC) v7.1
- ISO/IEC 27001:2022 and 27002:2022
- HIPAA – Federal Register 45 CFR Part 164, Subparts C, D, and E
- AICPA Trust Services Principles and Criteria: Security, Confidentiality, and Availability

HITRUST introduced version 11.7 of the CSF on December 18, 2025. The latest version includes 72 total authoritative sources, representing an increase of 20% from 2024.

Advancements in information technology shaped what assurance looks like today, but stakeholders require further evolution in assurance to meet their current needs.

Today's stakeholders need assurance providers who:

1. **Provide threat-intelligent assurance.**
   Stakeholders should know that the assurance mechanism has addressed the relevant threats for that organization.
2. **Maintain integrity.**
   The assurance process must report reliable results without the ability to circumvent its built-in integrity mechanisms.
3. **Reduce supply chain exposure.**
   Assurance mechanisms need to address the full scope, including those risk areas managed by the organization's third-parties.
4. **Offer AI assurance.**
   Assurance providers need to have AI assessments grounded in threat intelligence and governance controls.
5. **Deliver "good information security assurance."**
   This includes measurable results that can improve their security posture and adapt to emerging threats.



HITRUST provides each of these through the assurance processes and innovations described in this Trust Report.

Information Security Assurance: Present Day

Today, cyber threats continue to evolve and become more sophisticated while many of the legacy assurance providers have stopped adapting and innovating. Instead, a wave of new assurance providers are surfacing to deal with the areas of weakness left behind.

Information security assurance has developed into a global, multi-framework ecosystem, resulting in many options but a fragmented and confusing process for organizations who want to understand the best way to validate and improve their security posture.

The pressure on organizations to prove their security maturity has never been higher. Organization partners, customers, and other stakeholders are all looking for assurance that the security environment has been protected. Unfortunately, this has left organizations to:

Navigate the Maze.

Navigate a maze of overlapping standards and frameworks.

Manage Costs.

Manage the financial cost of multiple assessments that cover much of the same ground.

Prove Compliance.

Shoulder the stress and complexity of proving compliance over and over again.

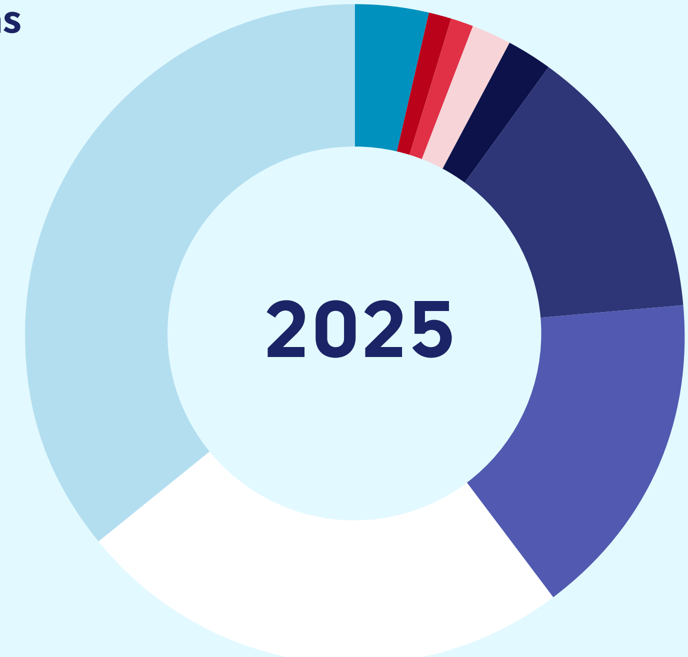
Instead of strengthening trust, this fragmented approach drains resources and slows progress.

Although HITRUST's mission began with protecting healthcare data, it evolved into a mission of harmonizing requirements to reduce duplicative efforts and create pathways toward mutual reciprocity across assurance providers.

HITRUST provides results which organizations of all types can trust while simplifying their assurance burden.

Active HITRUST Certifications By Industry

Industry	Share
Software & Technology	35.98%
Healthcare & Medical	24.50%
Business Services	16.18%
Financial Services	13.56%
Government	2.16%
Manufacturing	1.85%
Consumer Goods & Services	1.16%
Retail & Distribution	1.08%
Other	3.53%

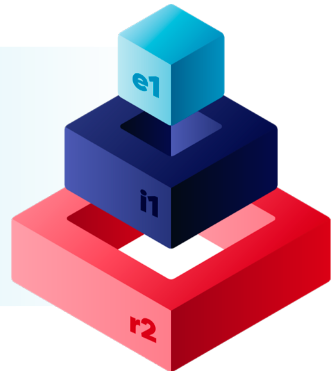


In order to serve multiple industries and organization sizes, HITRUST introduced several certification types, ranging from 43 requirements in the HITRUST e1 assessment to the variable assessment size of the HITRUST r2 assessment. When an organization performs an r2 assessment, it first completes a risk analysis to ensure the assessment is tailored to provide the necessary HITRUST requirements to reach the highest level of assurance. In 2025, HITRUST noted that an r2 validated assessment averaged 387 requirements, which reflects a slight increase from the average of 379 requirements in 2024.

HITRUST Certification Types

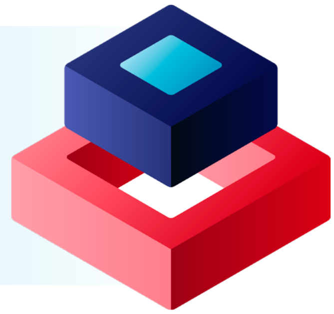
The HITRUST e1 assessment is a one-year certification which provides entry-level assurance focused on the 43 most critical cybersecurity controls and demonstrates that essential cybersecurity hygiene is in place.

e1



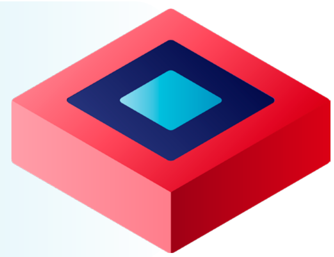
The HITRUST i1 assessment is a one-year certification which addresses 182 cybersecurity leading practices and a broader range of active cyber threats than the e1 assessment while providing a moderate level of assurance.

i1



The HITRUST r2 assessment is a two-year certification which provides the highest level of assurance focused on a comprehensive specification of controls based on data volumes, regulatory compliance, and other risk factors.

r2



The NIST Cybersecurity Framework (CSF) certification is presented via HITRUST's NIST CSF Scorecard. The Scorecard reflects the aggregated scores for the underlying HITRUST CSF controls as they are mapped by HITRUST to the NIST Cybersecurity Framework Core Subcategories.

NIST CYBERSECURITY FRAMEWORK

The HITRUST AI Security Certification was one of the first AI certifications on the market, developed with input from AI industry experts. It focuses on addressing the AI security threats which accompany the deployment of AI within an organization. The HITRUST AI Security Certification consists of up to 44 additional HITRUST requirements in an assessment (exact number is dependent on the results of the HITRUST AI risk analysis).

AI SECURITY

HITRUST Insights Reports

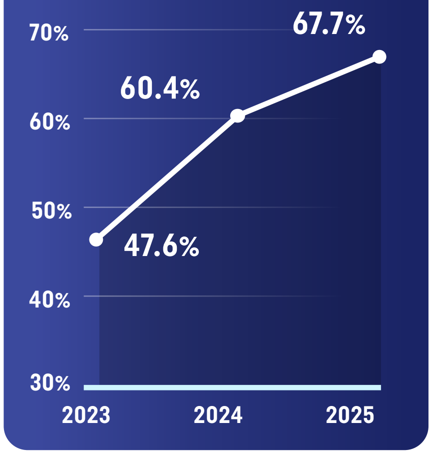
HITRUST expanded its Insights Report offerings in 2025 by 267%, now offering 11 report types. The report types added in 2025 include GovRAMP, CMMC, NIST 800-171 and Ransomware[11].

Organizations may select one or more authoritative sources which incorporates that source's requirements into its HITRUST assessment. This allows an organization to assess its security posture alongside a selected standard or regulation. Several of these sources are also able to generate a *HITRUST Insights Report*.

HITRUST Insights Reports provide easy-to-understand and reliable reports which may be shared with internal and external stakeholders to illustrate the organization's control maturity in a clear and concise format. An Insights Report includes the testing results for HITRUST requirements in an assessment based on selecting an eligible source (e.g., HIPAA), providing an independent perspective on the organization's conformity. This may be particularly valuable for stakeholders who need their vendors to demonstrate compliance with a particular framework or standard.

In 2025, almost 68% of new HITRUST customers selected the e1 assessment. This supports our expectation when we introduced the e1 assessment that it would act as an entry level assessment to allow companies to start building a foundation of a strong information security program. This trend has continued over time as the percent of new customers selecting the e1 has grown 20% since 2023.

Adoption of e1 Assessments by New HITRUST Customers

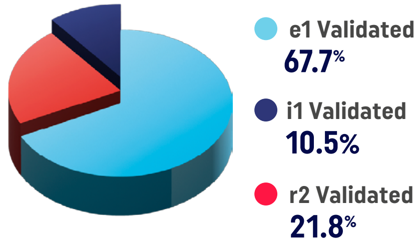


For all current active certifications as of December 31, 2025, the HITRUST r2 assessment is still performed by the majority of HITRUST customers as over two-thirds of HITRUST customers maintain an active r2 certification.

HITRUST continues to iterate and innovate on its framework and assurance processes to increase the relevancy and reliability of its certification for organizations and their stakeholders. In the next chapter, we will review a key innovation which keeps the CSF current even as the information security landscape shifts: **HITRUST's CTA capability.**

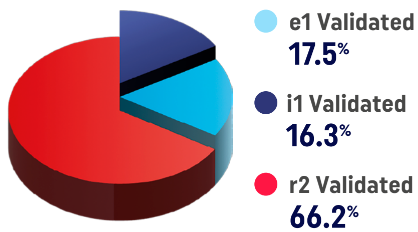
New Customers by Assessment Type

The HITRUST e1 assessment acts as an entry-level assessment, allowing companies to build the foundation of a strong information security program.



Active HITRUST Certifications by Assessment Types

Over two-thirds of HITRUST customers maintain an active r2 certification.



HITRUST CSF

While more than 40% of organizations report experiencing a breach, the breach rate for HITRUST-certified environments has continued a multi-year trend of exceptionally low breach rates.

HITRUST Cyber-Threat Adaptive (CTA) Capability

The evolution of the HITRUST CSF in recent years reflects some of the most significant advancements in the framework's history. With the release of HITRUST CSF v11, HITRUST undertook a comprehensive, data-driven review of real-world cyber threat intelligence mapped directly to the HITRUST CSF. Through this analysis, HITRUST established relationship mappings between CSF requirement statements and the adversarial techniques identified in *MITRE ATT&CK*, enabling a more precise understanding of how each requirement contributes to mitigating actual threats.

As a result of this ongoing evidence-based process, the CSF is continuously refined to ensure that every requirement included in the framework serves a clearly defined security purpose. Certain requirements are enhanced or newly introduced to address emerging techniques, while others are repositioned for inclusion only in assessments that incorporate corresponding authoritative sources. This systematic approach represents a deliberate departure from traditional, slower-moving frameworks that rely on consensus-driven processes[12]. Instead, HITRUST grounds its requirements in threat-focused intelligence to maintain ongoing relevance in an environment where adversary tactics continually evolve.

In addition to this methodical approach to developing the CSF, one of HITRUST's key innovations which has allowed it to maintain a relevant assessment is the Cyber-Threat Adaptive (CTA) capability within the HITRUST CSF.

> HITRUST continuously reviews the threat intelligence data to ensure the HITRUST CSF is addressing the latest critical threats.

CTA enables informed updates to all HITRUST assessments, ensuring the necessary information security coverage based on objective threat intelligence rather than subjective judgment.

This approach to the HITRUST CSF design allows:

1. **The provision of prescriptive requirements to address current cyber threats.**
2. **The ability to quickly respond and adapt the HITRUST CSF as new technologies (and cyber threats) arise.**

MITRE ATT&CK

The MITRE ATT&CK framework details the various methods or techniques that adversaries operate during a cyber attack. MITRE has identified various mitigations to prevent or significantly hinder an attacker from successfully executing that technique.

- The HITRUST CSF provides coverage for 100% of the MITRE-published cyber attack techniques that can be mitigated.
- The HITRUST e1 assessment includes requirements which provide coverage for 97.3% of the attack techniques that can be mitigated.
- The HITRUST i1 and r2 provide coverage for 100% of the attack techniques that can be mitigated.

2025 Top Threat Actions

The Verizon 2025 DBIR describes the common actions threat actors are using in breaches and incidents. The Verizon 2025 DBIR reported the top action variety in breaches was ransomware (44% of reported breaches), while the top two action vectors used in breaches were web applications and email, used in 34% and 27% of breaches respectively, demonstrating the importance of securing both of those attack vectors.

> All HITRUST assessments require ransomware coverage with preventive tools, multi-factor access controls, offline backups, and training activities.

HITRUST regularly publishes a CSF Threat & Mitigation Analysis[13] to confirm that our i1, e1, and r2 requirement selections are responsive to the current threat landscape. As part of each analysis, we review real-world breaches, threat indicators, and mappings to MITRE ATT&CK techniques and mitigations. This is necessary since cyber threats evolve rapidly, and static or slow-moving assurance providers may struggle to remain effective.

Cyber threats evolve rapidly, and static or slow-moving assurance providers may struggle to remain effective.

Based on our CTA threat coverage data, we identified the top five requirement statements in percentage of addressed attack technique coverage within a HITRUST e1 assessment. The controls within these requirements protect against the highest number of attack techniques referenced in the MITRE ATT&CK framework. Four of the top five requirements are in the Access Control domain, highlighting its particular importance in mitigating adversarial attacks.

Domain	HITRUST Requirement Statement	% of Attack Technique Coverage
11 Access Control	The allocation of privileges for all systems and system components is controlled through a formal authorization process. The organization ensures access privileges associated with each system product (e.g., operating system, database management system, and each application) and the users associated with each system product which need to be allocated are identified. Privileges are allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy (e.g., the minimum requirement for their functional role-user or administrator, only when needed).	37.5%
11 Access Control	The organization reviews all accounts (including user, privileged, system, shared, and seeded accounts), and privileges (e.g., user-to-role assignments, user-to-object assignments) periodically (annually at a minimum).	30.6%
11 Access Control	The organization limits authorization to privileged accounts on information systems to a predefined subset of users and tracks and monitors privileged role assignments.	30.6%
08 Network Protection	Security gateways (e.g., a firewall) are used between the internal network, external networks (Internet and third-party networks), and any demilitarized zone (DMZ). An internal network perimeter is implemented by installing a secure gateway (e.g., a firewall) between two interconnected networks to control access and information flow between the two domains. This gateway is capable of enforcing security policies, being configured to filter traffic between these domains, and blocking unauthorized access in accordance with the organization's access control policy. Wireless networks are segregated from internal and private networks. The organization requires a firewall between any wireless network and the covered and/or confidential information systems environment.	23.1%
11 Access Control	Each user ID in the information system (including non-privileged, privileged, seeded, and service accounts) is assigned to a specific, named individual to maintain accountability.	17.1%

Other assurance providers are typically less prescriptive in their framework design, allowing the customer to determine the specific controls to implement. This approach imparts much of the responsibility (and burden) for detailed control selection to the organization and its assessors. While it offers customers flexibility in their implementation, this also introduces a situation where:

- An organization may only perform the minimum necessary to achieve the assurance report rather than identifying and implementing the appropriate security protections for their environment.
- An organization, without specific guidance, may also incorrectly assess their risks, resulting in an incomplete selection of controls and continued exposure to specific threats.

For these reasons it becomes challenging for a stakeholder to truly understand the security posture for their vendors, service providers, or customers when receiving one of these assurance mechanisms, further contributing to the current Trust Crisis.

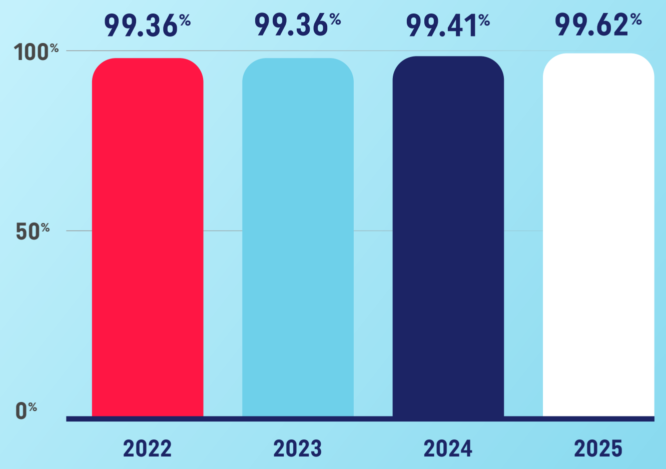
> The approach taken by other assurance providers imparts much of the responsibility (and burden) for detailed control selection to the organization and its assessors.

HITRUST Breach Rate

HITRUST's innovative Cyber-Threat Adaptive approach continues to produce relevant certifications which are meaningful for stakeholders. Many other assurance providers have fallen short due to their inability to commit resources toward ensuring their framework addresses current threats. However, it is clear the process HITRUST has put forth continues to work.

> 99.62% of HITRUST-certified environments did not report a security breach in their certified platforms in 2025.

HITRUST Breach-Free Rates



The percentage of reported breaches by HITRUST-certified environments over time

As noted in the chart, the breach rate for HITRUST-certified environments has remained consistently low. Over the prior four years, only 0.56% of HITRUST-certified environments have reported having a breach in their certified environment. HITRUST maintains three key processes to identify whether a HITRUST-certified environment experienced a security breach:

- All HITRUST-certified environments are contractually obligated to notify us when they have identified a security breach in their HITRUST-certified environment.
- External Assessors must examine with each organization and report to HITRUST whether the certified organization experienced a security breach upon the one-year anniversary of an r2 assessment (i.e., during the interim assessment).
- HITRUST proactively monitors publicly available sources to identify potentially unreported breaches from HITRUST-certified environments.

While there is no centralized repository to identify all security breaches, surveys, publicly available data, and required regulatory reporting, all provide insights into the number of companies experiencing data breaches:

- According to the UK Cyber Security Breaches Survey 2025[14], **43% of UK businesses surveyed experienced a security breach or attack** in the prior 12 months.
- According to the 2024 KPMG Cybersecurity Survey of C-suite cyber leaders at large companies (revenue greater than $1 billion)[15], **40% reported their company had suffered a recent cyberattack resulting in a security breach**.
- According to a 2025 Talker Research Survey of U.S. C-Suite and Direct Managers in Cyber Security[16], **43% of the companies surveyed have experienced a data breach**.
- According to Munich RE's Global Cyber Risk and Insurance Survey 2024[17], **47% of the interviewed companies had been affected by a cybersecurity breach**.

These reports consistently point to a breach rate of 40% or more across all companies, significantly higher than the breach rate of those with a HITRUST certification.

Healthcare Industry Breaches

The healthcare industry has always had a high share of security breaches due to the sensitive data managed by the industry. In 2025, it continues to be highly impacted by security breaches.

- According to the Kroll Data Breach Outlook 2025[18] healthcare was the most breached industry, accounting for nearly a quarter (23%) of breaches.
- According to IBM's Cost of a Data Breach Report 2025[19], the average cost of a healthcare breach was $7.42 million. The healthcare sector has been the costliest sector for a breach for 12 consecutive years.
- Healthcare breaches took the longest to identify at 279 days (five weeks longer than the global average)[20], contributing to the elevated costs of a breach.
- According to a Black Book Research Survey[21], 67% of security professionals at health provider organizations have experienced clinical disruption or downtime in the past 24 months due to a vendor outage or cyber event.

> **"Attackers continue to value and target the industry's patient personal identification information (PII), which can be used for identity theft, insurance fraud, and other financial crimes."**
>
> *– IBM Cost of a Data Breach Report 2025[2]*

Healthcare companies are required to report any breaches of PHI (Protected Health Information) to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR). OCR maintains a breach portal where they publish reported breaches affecting 500 or more individuals[23].

710 data breaches were published into the portal in 2025, impacting a total of 61,556,256 individuals.

As part of HITRUST's breach review process, HITRUST verified the top 50 breaches (by impacted individuals) did not occur in a HITRUST-certified environment.

HITRUST confirmed that none of the top 50 breaches in the OCR breach portal from 2025 occurred in a HITRUST-certified environment.

HITRUST MYCSF PLATFORM

While service providers are increasingly being used to breach organizations, over 80% of HITRUST certifications, including 100% of r2 certifications, addressed service provider threats.

HITRUST MYCSF PLATFORM

HITRUST developed the MyCSF platform to integrate all stakeholders into the system of Trust. The HITRUST MyCSF platform allows an organization to manage its assessment and certification process through coordination with its assessor, service providers, and HITRUST. MyCSF has become the central repository where customers work to document, communicate, and improve their information security performance. As a result of the capabilities of MyCSF, HITRUST is uniquely positioned to understand each organization's true information security maturity and provide the reporting that each organization requires.

MyCSF allows organizations to perform high-quality assessments against the HITRUST CSF utilizing the following innovations to produce reliable assessment results:

- **HITRUST CONTROL MATURITY & SCORING MODEL**
- **SHARED RESPONSIBILITY & INHERITANCE**
- **HITRUST ASSURANCE PROGRAM**

"Our innovation and investment into MyCSF enables organizations to use HITRUST as a centralized platform for managing and monitoring their information security performance and risks."

– Jeremy Huval, HITRUST Chief Innovation Officer

HITRUST Control Maturity and Scoring Model

Real-world cybersecurity is rarely black and white but instead exists along a continuum of maturity and performance. Acknowledging this reality, HITRUST developed an innovative PRISMA-based control maturity and scoring model. Unlike other assurance providers that rely on binary pass-or-fail determinations, the HITRUST scoring model reflects modern risk management by recognizing varying degrees of control maturity and effectiveness. This more nuanced, risk-based approach provides organizations with a clearer, more actionable understanding of their security posture.

The HITRUST scoring model uses a scoring rubric to assist External Assessors with their scoring evaluations. All validated assessments submitted to HITRUST utilize the HITRUST scoring model to evaluate the organization's control maturity. Upon submission, the MyCSF platform performs all the necessary calculations to determine an organization's results, including whether it achieved certification and any required *Corrective Action Plans (CAPs)* for HITRUST requirements which did not achieve the required score.

In order to achieve a HITRUST certification, each HITRUST domain must achieve a score that meets or exceeds the certification threshold for the assessment type selected. The e1 and i1 require the core requirement statements in each domain to achieve a score of at least an 83, while the r2 requires each domain to score at least a 62 to achieve certification. The difference in the certification thresholds is attributable to the optional inclusion of the Measured and Managed maturity levels in an r2, where the e1 and i1 assessments do not include those maturity levels.

In the table below, HITRUST identified the lowest scoring domains by assessment type. For the r2 and i1 assessments, organizations have consistently struggled with managing Data Protection & Privacy across the previous three years. This domain includes being able to identify, manage, and encrypt all sensitive data within the company.

Corrective Action Plans (CAPs)

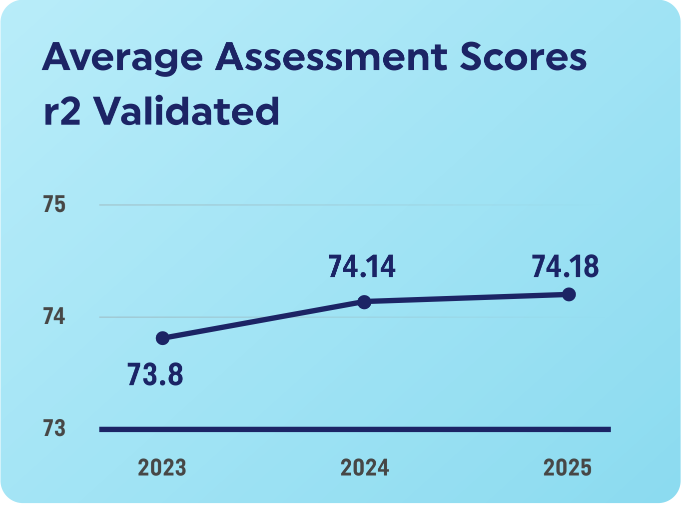
When an organization has not fully implemented certain HITRUST requirement(s) but still achieves certification, this may result in a "Corrective Action Plan" (CAP) for the corresponding HITRUST requirement(s). HITRUST expects organizations to make annual progress on these CAPs to address those weaknesses in their security environment and continually improve their cyber resilience capabilities. HITRUST reviews an organization's CAP progress within an r2 assessment when the organization performs its interim assessment.

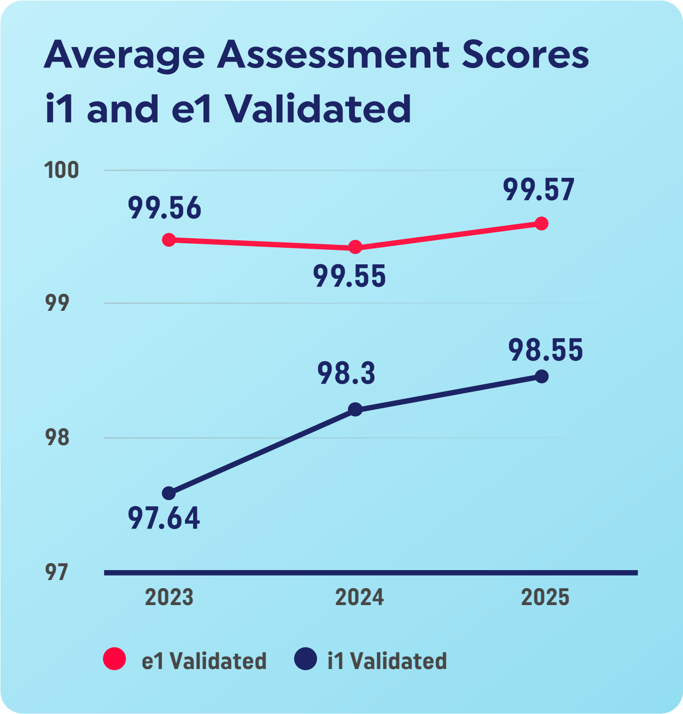
> For the third year in a row, the lowest scoring domain in the e1 assessment was *Access Control*. It is important for organizations to get this right as the Verizon 2025 DBIR saw attacks using "Credentials" as the most common path for attackers to initiate a breach.

Lowest Scoring Domains by Assessment Type

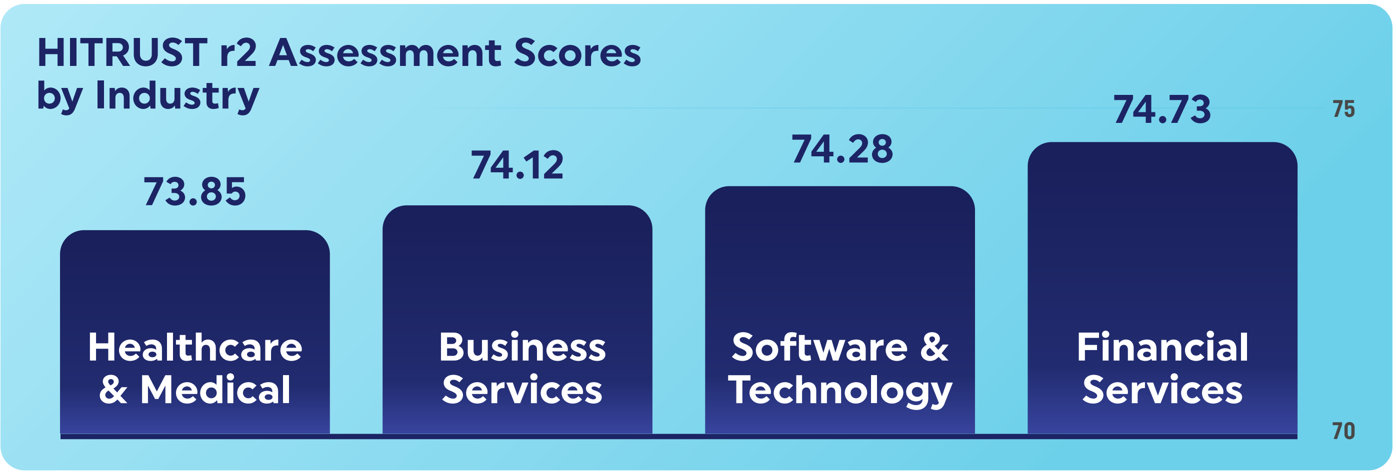
	HITRUST r2 Validated Assessment	HITRUST i1 Validated Assessment	HITRUST e1 Validated Assessment
2025	Data Protection & Privacy	Data Protection & Privacy	Access Control
2024	Data Protection & Privacy, Password Management (tied)	Vulnerability Management	Access Control
2023	Password Management	Data Protection & Privacy	Access Control

When looking at the overall average scores for each assessment type, HITRUST has seen a slight but consistent increase over the prior three years, reflecting general improvements in security maturity[24].





We found a larger variation when looking at scores by the top four industries with HITRUST r2 certifications. Unsurprisingly, Financial Services continues to have the highest information security maturity scores. However, the Healthcare industry is lagging behind other sectors, scoring lower than the overall average assessment score of 74.20 and lower than Financial Services by almost a point.

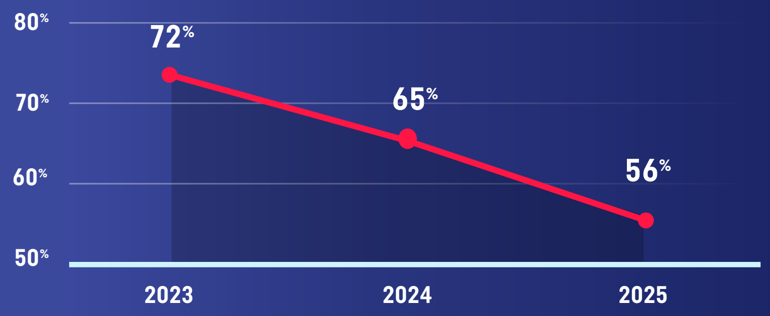


The Healthcare industry is lagging behind other sectors, scoring lower than the overall average assessment score of 74.20 and lower than Financial Services by almost a point.

Demonstrating Improvement in Information Security

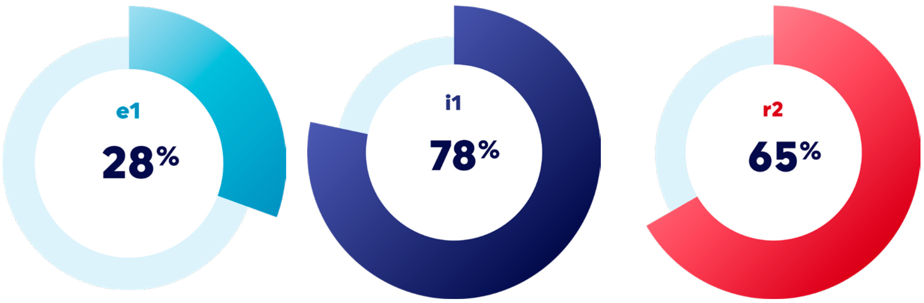
Organizations and their stakeholders have a strong need to ensure weaknesses in the organization's threat coverage are well understood and either corrected or mitigated. HITRUST attaches CAPs to specific HITRUST requirements when there are controls expected to be remediated by the organization. The remediation of CAPs contributes to the continual improvement of a HITRUST certification holder's security posture. We continued to see a reduction in assessments with CAPs on a year-over-year basis overall with 9% fewer HITRUST assessments having CAPs in 2025 than 2024 across all assessment types.

2025 Validated Assessments with One or More Corrective Action Plans (CAPs)



When broken down by assessment type, we found that the number of r2 and i1 assessments with CAPs decreased between 2024 and 2025, with the **r2 assessments with CAPs decreasing by 3.6% (68.6% to 65%) and the i1 assessments with CAPs decreasing by 10.5% (88.5% to 78%) since last year.** The e1 assessment noted a slight increase of 1.5% from 2024, but remained the lowest of all assessment types with only 28% of e1 assessments having one or more CAPs.

2025 Validated Assessments with CAPs by Assessment Type



Are Your Third-Party Security Holes Being Addressed?

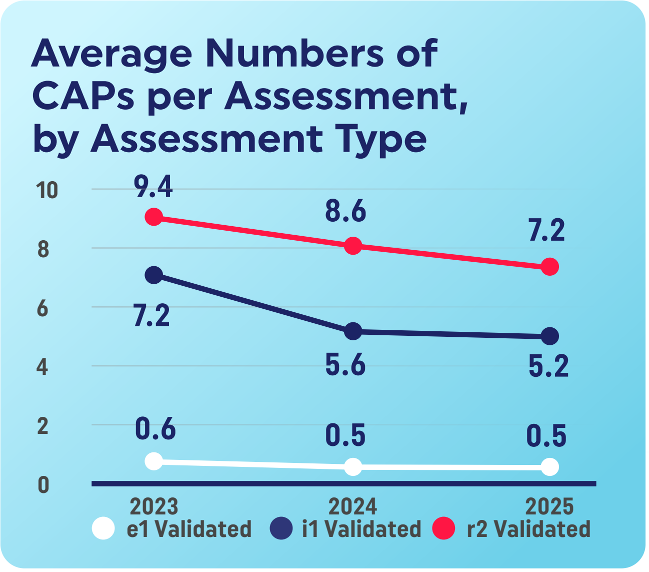
It is by design that HITRUST assessments show consistent improvement, as reflected in the diminishing number of corrective actions required on a year-over-year basis. HITRUST expects organizations to make annual progress on remediating these CAPs and monitors their closure in r2 interim assessments.

In many other assurance reports, there is no tracking of these exceptions and their remediation by either the assurance provider or firms issuing the reports. With improvement at the discretion of each organization, it's not an easily workable solution for stakeholders relying on those reports to track progress or overall improvement data on their third parties.

> Stakeholders receiving HITRUST reports from their third-parties can be confident the identified security holes are consistently closed.

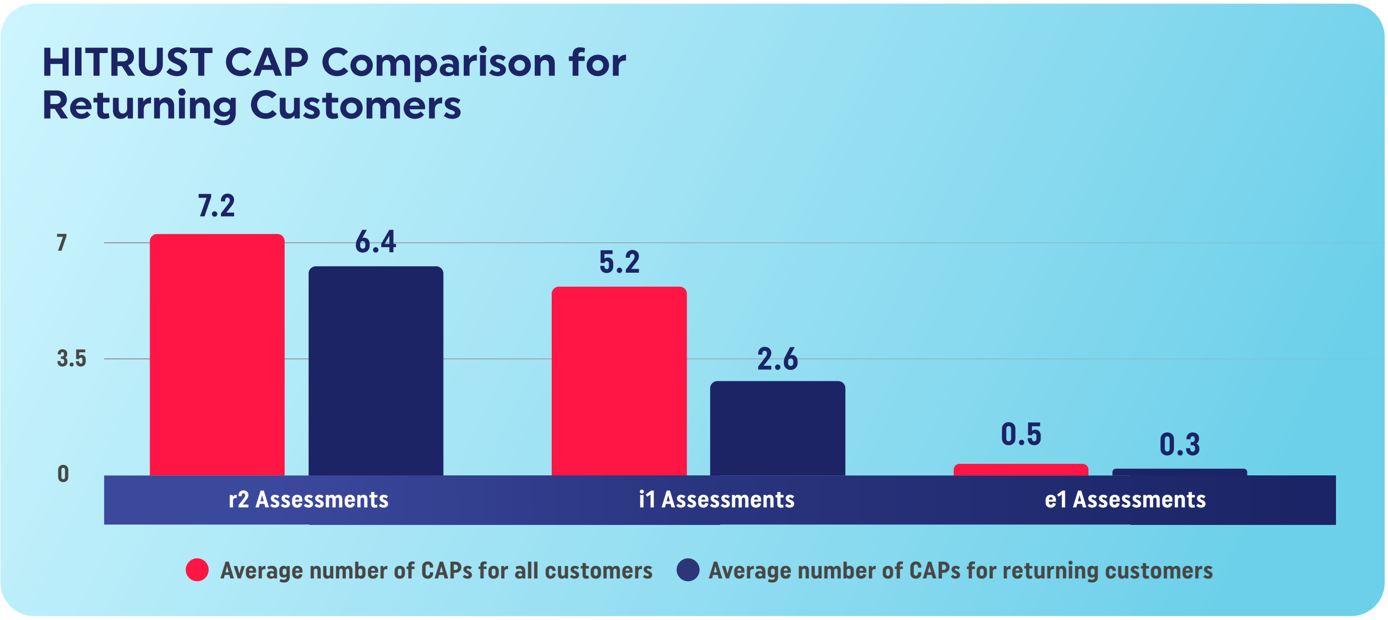
We continued to see improvement in the average number of CAPs per assessment for the r2 and i1 on a year-over-year basis, while the e1 held steady at the low average of half a CAP per assessment.

The r2 remained the assessment type with the highest average number of CAPs which is to be expected with the larger assessment size. Since assessment size can influence the number of CAPs in an assessment, we also inspected how frequently a CAP occurs in each assessment type. Upon analysis of the average number of CAPs compared to the number of requirements in each assessment type, CAPs occurred most frequently in the i1 assessment, at a rate of 2.9%. CAPs occurred in the r2 assessment at a rate of 1.9% while the e1 remained the lowest at 1.1%.



The high CAP rate in the i1 along with the high percentage of i1 assessments which included CAPs (77%) suggests that organizations performing i1 assessments, on average, have required more improvements in their security posture than other organizations.

However, we also identified the i1 assessment includes the most dramatic reduction in CAPs for returning HITRUST customers, when compared to the average number of CAPs for all customers. We observed 50% fewer CAPs for returning i1 customers, with e1 returning customers averaging 40% fewer CAPs and r2 returning customers averaging 11% fewer CAPs.



When analyzing the five HITRUST requirements which had the most CAPs in 2025, we found that three of the top five were also in the 2024 top five, indicating a continued struggle for organizations to address these requirements internally. It appears to be of particular significance that organizations continue finding challenges with performing periodic third-party Service Level Agreement (SLA) reviews, which are expected to enforce the organization's expected information security requirements within their supply chain.

HITRUST Requirements Causing the Most Corrective Action Plans (CAPs) in HITRUST Assessments

2025 Ranking	2024 Ranking	HITRUST Domain	HITRUST Requirement ID	HITRUST Requirement Description	HITRUST Requirement Summary
1	7	Access Control	11.01e1System.2	The organization reviews all accounts (including user, privileged, system, shared, and seeded accounts) and privileges (e.g., user-to-role assignments, user-to-object assignments) periodically (annually at a minimum).	Periodic user access reviews
2	1	Third Party Assurance	1411.09f1System.1	The organization ensures a periodic review of service-level agreements (SLAs) is conducted at least annually, and compared against the monitoring records.	Periodic third-party SLA reviews
3	5	Access Control	11.01p1System.5	A policy applicable to the organization's information systems addressing account lockout after consecutive unsuccessful login attempts are documented and enforced through technical controls.	Account lockout upon consecutive failed logins
4	3	Audit Logging & Monitoring	12101.09ab1System.2	The organization specifies how often audit logs are reviewed, how the reviews are documented, and the specific roles and responsibilities of the personnel conducting the reviews, including the professional certifications or other qualifications required.	Periodic audit log reviews
5	N/A	Information Protection Program	0183.07b1Organizational.1	All information systems are documented. Documentation of all information systems includes a method to determine accurately and readily the: assigned owner of responsibility; owner's contact information; and purpose (e.g., through labeling, coding, and/or inventory).	Information System accountability

Shared Responsibility and Inheritance

> **"It is not a good strategy to just sit around and check the news to see if you won the vendor lottery that day."**
>
> *- Verizon 2025 Data Breach Investigations Report*

Adversaries have identified that security weaknesses in an organization's third parties can provide a path into their actual target organization[25]. Despite these rising supply chain attacks, organizations have a business need to continue, and increase, their reliance on service providers. They are a necessary component for many businesses to provide efficiency and leverage necessary services.

The surge in supply chain attacks coupled with the business need to expand service provider reliance creates a cycle where we expect to continue seeing supply chain attacks proliferate.

The HITRUST r2 assessment requires organizations to directly score and validate all requirements performed by their service providers. To assist organizations with identifying those requirements which should be scored for service providers, HITRUST offers a baseline shared responsibility matrix (SRM) along with 15 service provider SRMs covering all major Cloud Service Providers (CSPs).

HITRUST allows the exclusion (i.e., carve-out) of service providers in e1 and i1 assessments for situations where an organization is unable to address the risks posed by their service providers. However, even with exclusion, only 16.9% of i1 certifications and 13.9% of e1 certifications (with service providers in scope) excluded one or more of those service providers from the assessment.

Many other assurance reports do not include third parties due to complexities with that assurance provider's validation process.

> **HITRUST has simplified the service provider assessment process through a unique innovation called Inheritance.**

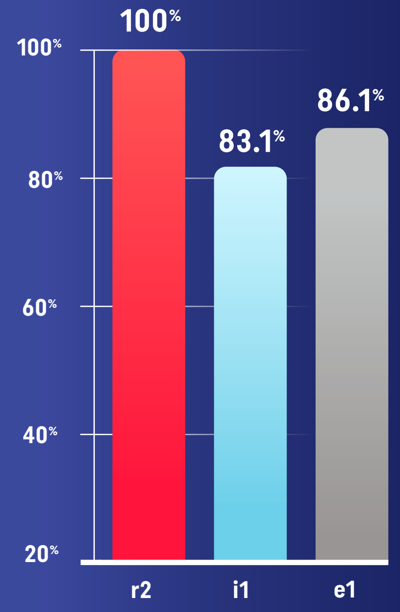
Do You Have a Third-Party Blind Spot?

Even with these intensifying attacks, most legacy assurance providers do not require an organization's service providers to be directly tested as part of the assessment. Instead they rely on organizational controls around vendor oversight and third party agreements.

Other assurance mechanisms allow an organization to choose whether to include or carve-out (exclude) service providers from scope. Due to the complexities in assessing those service providers, most organizations choose to exclude the service providers from testing. For stakeholders relying on assurance, this can cause a blind spot in the visibility of an organization's vendor security posture.

HITRUST's inheritance innovation simplifies this process, resulting in 100% of r2 assessments and over 80% of i1 and e1 assessments validating service provider performance.

HITRUST Third Party Coverage



Percentage of HITRUST assessments which tested all of the organization's service providers.

Efficiency Gains Using Inheritance

No other assurance provider has an inheritance functionality in their assessment process. In addition to providing increased security coverage over an organization's service providers, inheritance simplifies the assessment process, making it quicker and easier to achieve certification when inheritance is used.

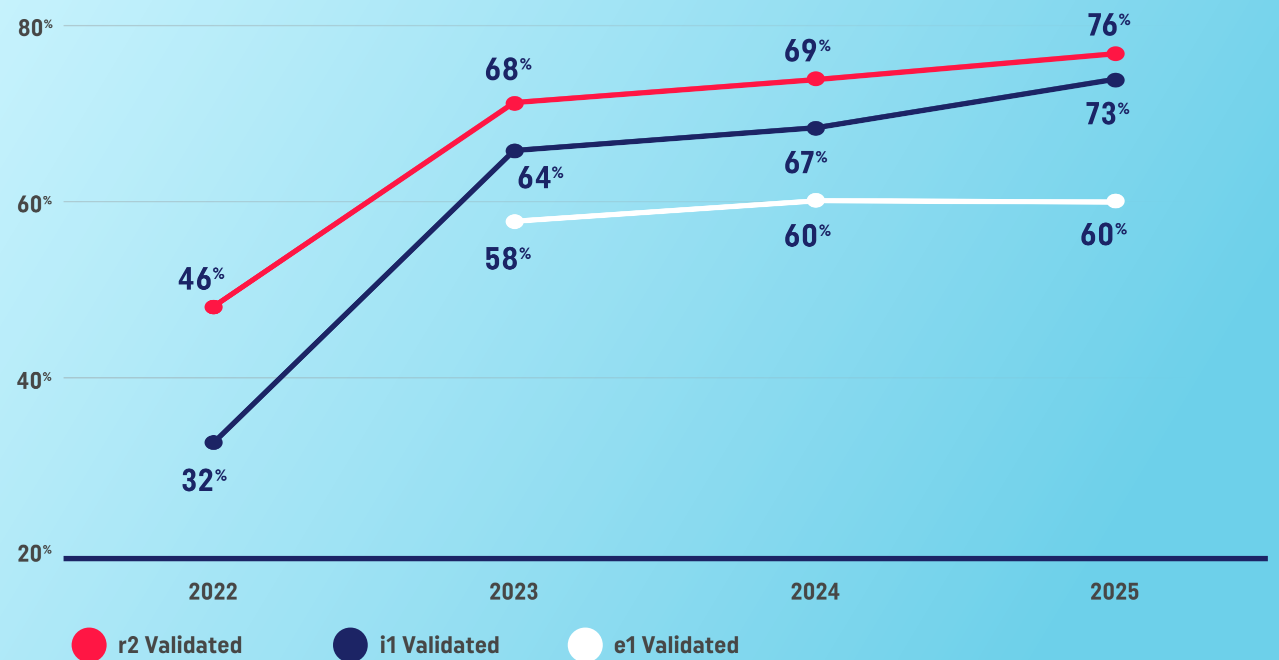
When comparing assessments which did not utilize inheritance to those which did utilize the inheritance functionality, we identified that External Assessors spent 11.4% fewer hours when the inheritance functionality was used, including:

- **19.6% fewer hours on r2** assessments which used the inheritance functionality.
- **35.5% fewer hours on i1** assessments which used the inheritance functionality.
- **2.4% fewer hours on e1** assessments which used the inheritance functionality.

Inheritance allows organizations to reuse inheritable controls from external third-party organizations and from their other HITRUST assessments. The inheritance functionality seamlessly incorporates the validated controls of their service providers into their own HITRUST assessments through a request and approval process. Controls can be inherited from vendors, major CSPs and an organization's existing HITRUST assessments.

In 2025, we continued to see a year-over-year increase in the use of inheritance in HITRUST assessments with over two-thirds (69.7%) of validated assessments utilizing External Inheritance, an increase of 5.6% from 2024 (64.1%).

Validated Assessments Using Inheritance by Assessment Type



HITRUST ASSURANCE PROGRAM

While CPAs have concerns about SOC quality and objectivity[26], HITRUST ensures these principles by requiring 100% of HITRUST assessments to undergo centralized & independent HITRUST quality review.

HITRUST Assurance Program

When developing the HITRUST framework and assurance processes, we understood the importance of having appropriate quality gates governing the production of each certification. As a result, HITRUST has focused its assurance and quality processes to ensure the highest level of integrity and confidence in a HITRUST certification. The HITRUST Assurance Program has several layers, including:

- HITRUST Automated Assurance Intelligence Engine (AIE) and Pre-Submission Review
- HITRUST Post-Submission Assessment Review
- Report Quality Process
- Escalated QA Process
- External Assessor Program
- Continuous Quality Monitoring

> **The HITRUST Assurance Program provides a granular level of oversight through a quality control process that reviews 100% of submitted assessments and issued certification reports.**

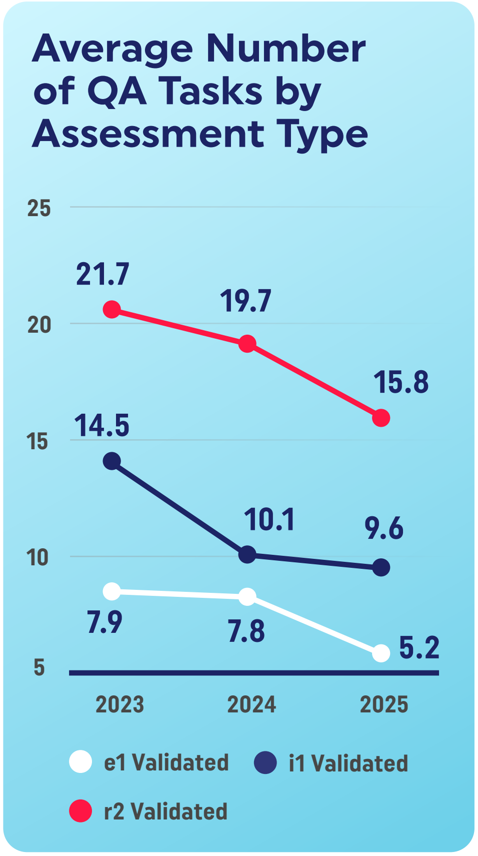
Each validated assessment must undergo a detailed quality assurance (QA) review by a HITRUST QA Analyst after it has been submitted to HITRUST. During the QA review, the HITRUST QA Analyst will review each potential quality issue, ensure the assessment information meets HITRUST criteria defined in the *HITRUST Assessment Handbook*, and perform an in-depth review of the testing performed by the External Assessor for a sample of requirement statements. The HITRUST QA Analyst will create QA tasks in the MyCSF platform, assigned to the organization or External Assessor, when questions or concerns are identified.

On a year-over-year basis, we found fewer QA tasks opened across the assessment types as noted in the chart, indicating further maturity and understanding of the expected approach by External Assessors when performing a HITRUST assessment.

HITRUST Assessment Handbook

HITRUST's robust assessment approach, control maturity and scoring methodology, and related assurance requirements are clearly articulated in the publicly available HITRUST Assessment Handbook (**hitrustalliance.net/assessment-handbook**). The HITRUST Assessment Handbook defines the criteria and processes for organizations and their assessors who are validating their information protection programs against the HITRUST CSF through a validated assessment.

The HITRUST Assessment Handbook was updated to version 1.2 on January 13, 2026, with additional information on potential certification statuses and guidance for testing evidence completeness and accuracy.



In 2025, the following were the top two types of tasks opened by HITRUST QA:

- 16% of tasks were related to assessment firms marking HITRUST requirements as Not Applicable (N/A). In these cases, our QA process ensures that the HITRUST requirements were appropriately tested and not avoided by indicating they were not applicable to the organization.
- 15% of tasks were related to the scope of the assessment. Our QA process is opening these tasks to ensure that an organization has correctly defined its scope within the assessment according to the HITRUST criteria[27].

To ensure consistency and accuracy in the QA feedback to organizations and their external assessors, HITRUST's Quality department independently reviews the performance of all HITRUST QA Analysts on a monthly basis. During its review, the HITRUST Quality team reperforms the QA Analysts' assessment review to ensure they reached the appropriate conclusion consistent with the HITRUST Assessment Handbook. HITRUST saw consistent high quality in the QA Analyst's performance throughout 2025 as 93% of assessments reviewed had no quality concerns.

HITRUST Internal Quality Review of QA

Percentage of HITRUST assessments with no quality concerns

One of the reasons for today's Trust Crisis has been a lack of innovation across legacy assurance providers. Unwilling to accept the status quo, we are continually endeavoring to find different ways to enhance HITRUST's quality processes. A few of the key innovations over the last several years which are unique to other assurance providers include:

ASSURANCE INTELLIGENCE ENGINE (AIE)

RESERVATION SYSTEM

EXTERNAL ASSESSOR REPORTING DASHBOARDS

Does Your Third-Party Report Have Quality Issues?

Many legacy assurance providers have no visibility into the underlying assessment performed prior to issuance of their assurance reports. Their frameworks allow the assurance reports to be produced and distributed by the same firms which are performing the assessments. As a result, most of the underlying assessments for those legacy assurance providers will not go through quality procedures independent from the issuing firm.

HITRUST creates an average of 15.8 quality tasks (in the r2) for the External Assessor to action on every HITRUST assessment. These assessments are submitted to HITRUST by many of the same firms performing and issuing those legacy assurance provider reports.

> Those quality concerns being corrected in HITRUST assessments are going unanswered in any assurance reports not undergoing an independent and centralized quality review.

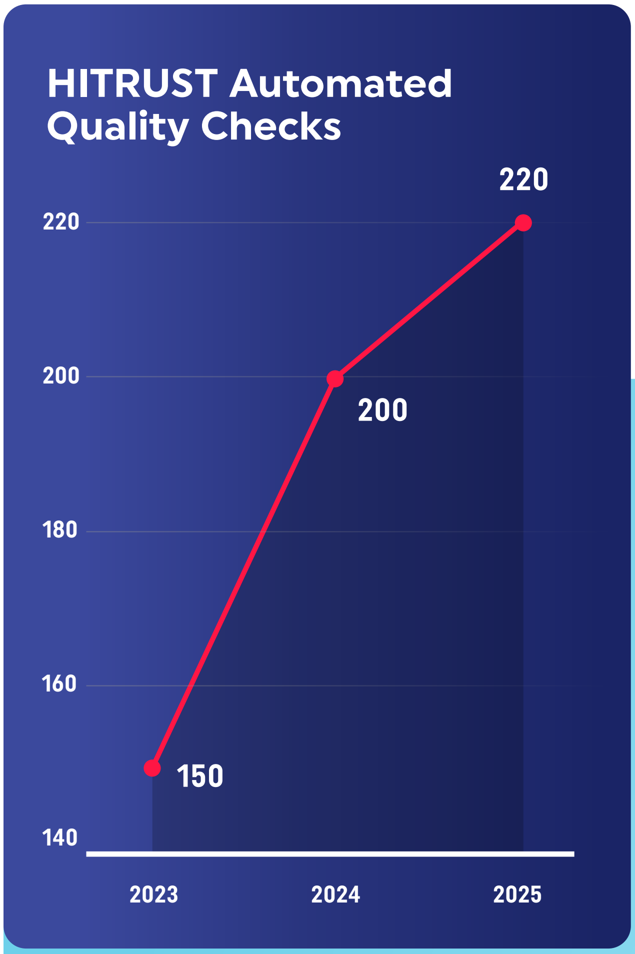
Assurance Intelligence Engine (AIE)

Since 100% of HITRUST assessments are submitted to us for quality review, it was important to build a tool which could quickly and efficiently identify quality concerns within an assessment. HITRUST developed the automated AIE within MyCSF to identify potential quality issues in real time during an assessment and upon assessment submission.

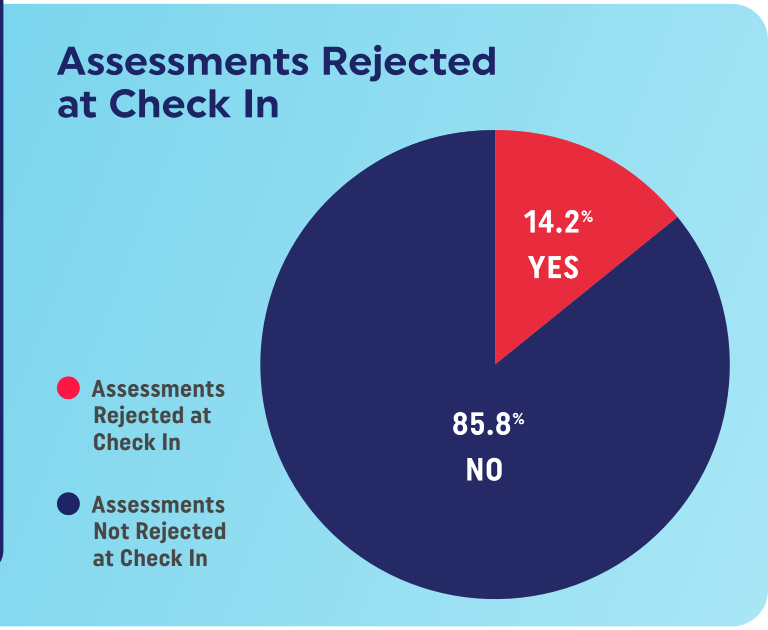
The AIE proactively identifies potential concerns by performing analysis against thousands of data points across the body of documentation for an assessment. When assessment firms are performing an assessment, the AIE provides them with detailed descriptions for potential quality issues, the triggering data point(s), and recommended remedial actions.

Upon submission, the assessment undergoes over 220 automated quality checks to identify and address assessment errors and omissions. Each year, HITRUST continues to advance the AIE with additional and smarter checks to automatically identify quality concerns.

HITRUST reviews each of the potential quality issues identified by the AIE and determines whether to accept the submission or return the submission to the External Assessor for remediation. In 2025, the AIE returned 14.2% of submissions back to the External Assessor for additional review of quality issues, representing a decrease of 7.3% from 2024.



Each year, HITRUST continues to advance the AIE with additional and smarter checks to automatically identify quality concerns.



Reservation System

HITRUST uses a centralized issuance model for all issued reports and certifications. Since HITRUST manages the assessment process and report issuance through the MyCSF platform, we developed an efficient process for managing the queue of submitted assessments; the automated Reservation System. The Reservation System allows organizations to schedule the start of their QA prior to submitting a HITRUST validated assessment. The Reservation System is designed to:

- Eliminate the uncertainty around when HITRUST's QA procedures will begin
- Allow organizations and their External Assessor to schedule resources to respond to HITRUST's QA feedback
- Provide the opportunity for QA to occur closer to the submission date

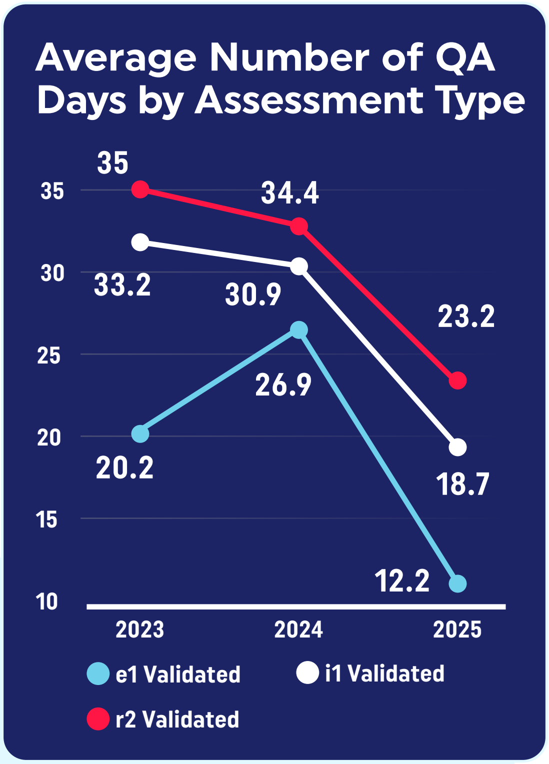
Since implementation of the Reservation System in 2021, HITRUST has observed a substantial decrease in the number of days after submission when an organization will receive their HITRUST report. As the MyCSF platform automatically records the amount of time a validated assessment resides within each phase of the workflow, HITRUST identified the average number of days from QA to draft report was lower from 2024 to 2025 across all assessment types.

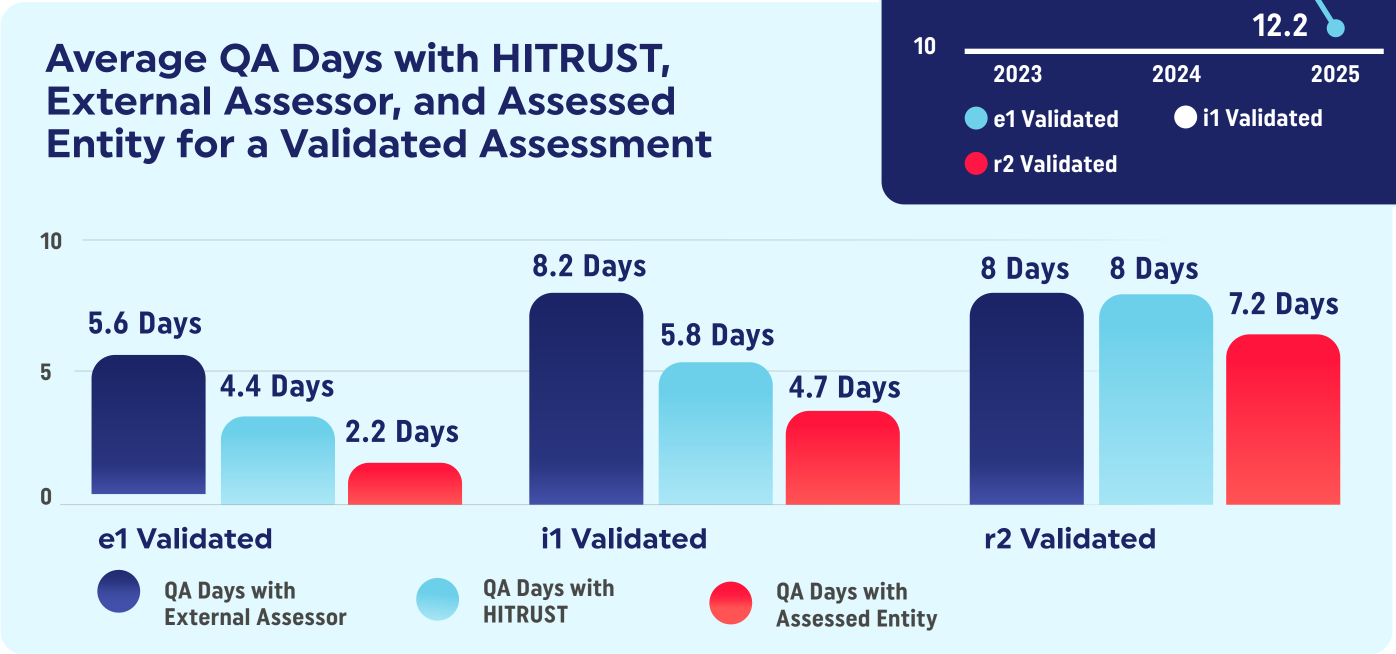
The average time for HITRUST to perform QA remains much lower than our SLAs. In 2025, HITRUST did not exceed the SLA threshold for any assessments.

Where Is My Report?

Many legacy assurance providers maintain a decentralized report issuance process, relying on other assessment firms or accreditation bodies to issue their reports. This can create uncertainty or inconsistency around an organization's timeline for receiving its assurance report.

HITRUST maintains a Service Level Agreement (SLA) of 30 days (with HITRUST) for the e1 and 45 days for the i1. If HITRUST does not meet the SLA, the organization's next e1 or i1 validated assessment report credit is complimentary. **This commitment is only possible through the consistency afforded by the HITRUST Reservation System.**





External Assessor Reporting Dashboards

All organizations must engage with a HITRUST-authorized External Assessor to perform validation procedures prior to completing and submitting a HITRUST validated assessment. Each External Assessor firm that wants to be in the HITRUST External Assessor Program must be vetted by HITRUST and utilize professionals trained and certified in the application of HITRUST's prescriptive assessment and assurance methodologies on every assessment.

In July 2025, HITRUST launched the External Assessor Reporting Dashboards within MyCSF. The dashboards provide External Assessors with specific data on their assessment performance. We expect this data will allow External Assessors to monitor and manage their performance more easily, resulting in improved consistency and quality across the community.

The External Assessor Reporting Dashboards include the following:

- Charts summarizing assessment performance, including number of drafts posted, average days in QA, hours spent per assessment type, and task types and volume.
- Trend charts comparing quarterly performance to other External Assessors and HITRUST targets.
- The current level of compliance with CCSFP and CHQP requirements including a report of active and expired CCSFP/CHQP practitioners associated with the External Assessor along with upcoming training dates.

For each submitted validated assessment, at least 50% of all engagement hours must be performed by practitioners with a CCSFP credential to ensure the team has an appropriate understanding of the HITRUST CSF and HITRUST Assurance Program methodologies and tools.
In 2025, over 85% of hours on each submitted validated assessment were performed by an individual with a CCSFP designation which represented a slight increase of 1% from 2024, but an 11% increase from 2023.

HITRUST's assurance program innovations continue producing high-quality, reliable assessments. When an assessment submitted to HITRUST is not high quality, it enters an Escalated QA process.

HITRUST Assessor Certifications

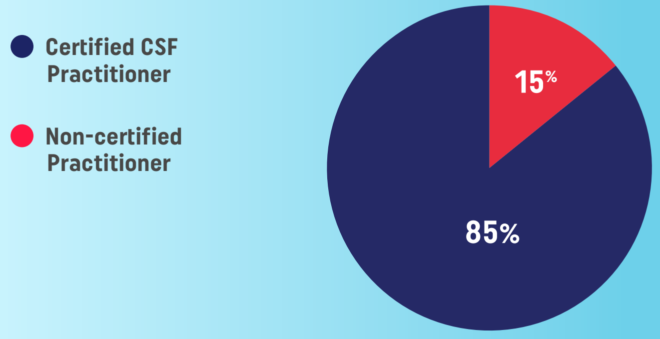
HITRUST offers two certifications for individuals to demonstrate their understanding of the HITRUST CSF and its information protection principles:

Certified CSF Practitioner (CCSFP) and Certified HITRUST Quality Professional (CHQP):

- **CCSFP:** Intended for individuals who plan to leverage the HITRUST CSF or External Assessors performing HITRUST assessments.
- **CHQP:** Provides guidance to practitioners expected to perform independent quality assurance (QA) reviews of validated assessment results.

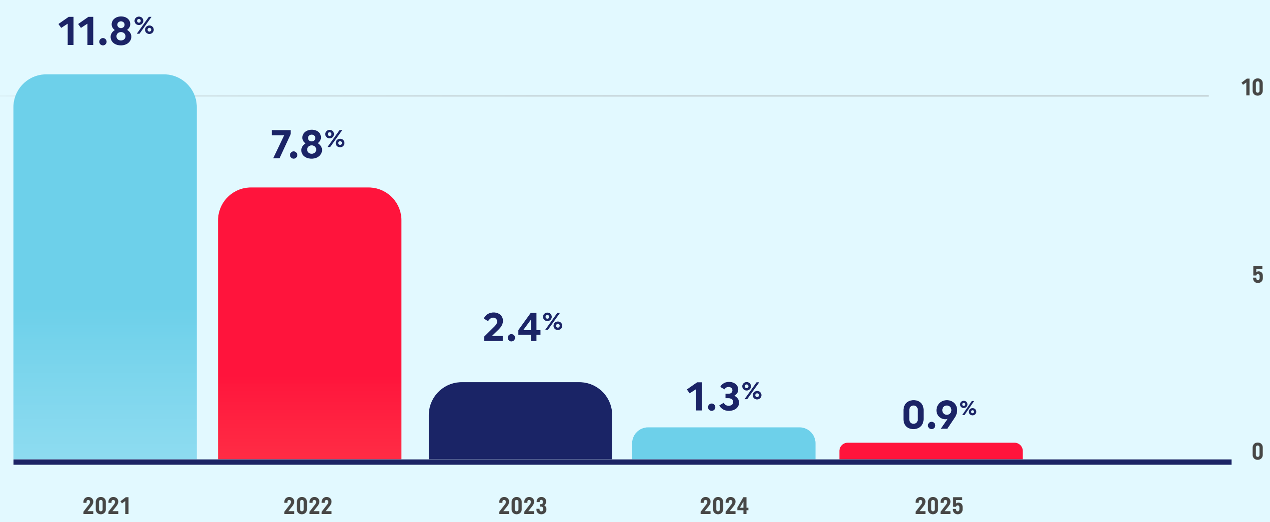
External Assessor firms must maintain a minimum of five practitioners with the CCSFP designation and two practitioners with the CHQP designation.

HITRUST Assessment Hours Incurred by CCSFP Certified vs. Noncertified Practitioners in 2025



The Escalated QA process is intended to identify and remediate issues found when an assessment does not meet the HITRUST criteria. Over the prior five years, we have seen a consistent reduction in the assessments which have entered Escalated QA. **This is a result of the consistent adaptation and iterations of our quality processes to achieve reliable certifications that organizations and their stakeholders can trust.**

HITRUST Assessments Entering Escalated QA Over Time



THE FUTURE OF TRUST

HITRUST is extending its threat-aligned assurance philosophy into two critical areas shaping the next era of risk: Artificial Intelligence and Third-Party Risk Management (TPRM).

Artificial Intelligence

As we move into 2026, governments and organizations are starting to ring warning bells around the need for further cybersecurity controls in AI:

- OpenAI warned that its upcoming artificial intelligence models could pose a "high" cybersecurity risk.
- A coalition of 42 U.S. state attorneys general sent a letter to major AI companies demanding better safety measures and rigorous testing for generative AI.
- Trend Micro has issued a warning about the rise of "vibe crime," where agentic AI is used to fully automate cyberattacks such as phishing, fraud, and data breaches, shifting criminal operations toward continuous, scalable, autonomous attack platforms.

As organizations adopt artificial intelligence across business functions, one of the most significant challenges they face is not the absence of controls, but uncertainty about which controls are necessary, where they should be applied, and how they should scale with risk. AI systems blur traditional boundaries between data, software, infrastructure, and decision-making, making it difficult for organizations to translate abstract AI risks into concrete, implementable control requirements.

HITRUST's AI Security Certification addresses this challenge by providing a structured, risk-based framework that helps organizations systematically identify the controls needed to deploy AI securely and responsibly. Rather than introducing an entirely new or isolated set of requirements, the certification extends established HITRUST CSF principles into AI-specific contexts, enabling organizations to build on familiar governance, security, and compliance practices.

HITRUST AI Security Certification

The HITRUST AI Security Certification, developed with input from AI industry experts, is one of the first AI certifications on the market and a continuation of the expansion of the HITRUST assessment portfolio.

The HITRUST AI Security Certification is designed to deliver an AI Security Assessment and accompanying certification for deployed AI systems. The HITRUST AI Security Assessment provides the same relevancy as other HITRUST certifications, as it includes a tailored set of AI security requirements encompassing fundamental security practices for deployed AI systems, addressing the relevant AI threats through analysis of multiple sources.

In 2026, HITRUST sees the AI threat landscape further expanding and companies starting to understand the risks which need to be addressed. HITRUST will leverage its CTA capability to continue adapting its framework for any emerging AI threats.

Third-Party Risk Management

Effective Third-Party Risk Management (TPRM) depends on assurance that is reliable, comparable, and aligned to real-world threats. As organizations increasingly rely on vendors, cloud service providers, and technology partners, TPRM programs must move beyond questionnaires and self-attestation toward assurance mechanisms that provide meaningful visibility into a third party's actual security posture. HITRUST is purpose-built to meet this need by delivering prescriptive, threat-informed, and independently validated assurance that can scale across complex and interconnected supply chains.

HITRUST certifications provide TPRM programs with confidence that a third party's security controls have been tested against a comprehensive and continuously evolving set of requirements grounded in observed threat activity. Unlike principle-based frameworks, HITRUST's Cyber-Threat Adaptive (CTA) capability ensures that assurance requirements evolve in direct response to attacker techniques and emerging risks, enabling TPRM teams to evaluate vendors based on current risk conditions rather than static criteria. Our centralized issuance process and mandatory quality assurance reviews (of 100 % of submitted assessments) further ensure consistent scoring, comparable results, and measurable risk reduction over time through standardized Corrective Action Plans (CAPs).

For stakeholders relying on vendor security, effective TPRM is ultimately about making faster, more confident risk decisions while reducing the operational burden of vendor due diligence. HITRUST enables those stakeholders to move away from fragmented, one-off assessments toward a shared assurance model that delivers consistent, threat-relevant insight across their third-party ecosystem. Because HITRUST certifications are standardized, independently validated, and continuously updated, organizations can trust that assurance results are comparable across vendors and aligned to current risk conditions.

This approach reduces duplicative assessments, accelerates onboarding and renewals, and allows TPRM teams to focus resources on vendors that present the greatest risk. At the same time, tracked Corrective Action Plans (CAPs) provide TPRM program managers with visibility into remediation progress over time, supporting continuous risk management rather than point-in-time compliance. By leveraging HITRUST, organizations gain a scalable, no-cost mechanism to improve due-diligence efficiency, reduce residual third-party risk, and strengthen confidence in the security of their supply chains.

Reliance Pitfalls

Many legacy assurance mechanisms were not designed to support the scale, consistency, or decision-making needs of modern TPRM programs. Other frameworks may rely on organization-defined controls mapped to general criteria, resulting in significant variability across reports and frequent gaps in baseline security practices.

As noted in this Trust Report, the absence of centralized oversight, real-time threat analysis, and third-party validation limits the effectiveness of many assurance reports as a decision-ready mechanism for organizations managing risk across large and diverse vendor populations.

In 2026, HITRUST is continuing to enhance those capabilities which enable TPRM program managers to more efficiently evaluate, monitor, and manage third-party risk.

These advancements are designed to further reduce friction in vendor risk management processes while improving visibility into supply chain risk, empowering stakeholders to identify, prioritize, and address third-party risk with greater speed, confidence, and consistency.

Closing Remarks

We believe that today's assurance providers have a responsibility to provide trustworthy assurance grounded in real-world threats, independent oversight, and measurable outcomes.

With the volume of companies and third-party stakeholders relying on assurance reports, assurance providers needed to continuously adapt and innovate to gain and maintain trust. Unfortunately, legacy assurance providers have become stagnant in their processes, resulting in the inability to adequately provide relevant assurances in a reliable report. Restoring this trust will require more than incremental updates to existing models. It will require a fundamental commitment to assurance that evolves at the pace of threats, scales across ecosystems, and delivers clarity rather than ambiguity to stakeholders.

Assurance that prioritizes flexibility over prescriptiveness, or self-attestation over validation, may offer convenience, but it does not reliably reduce risk. In contrast, assurance mechanisms that are threat-intelligent, data-driven, and centrally governed can produce measurable outcomes, including materially lower breach rates and demonstrable improvements in security maturity.

HITRUST was built on the belief that trust must be earned and sustained. Our framework, assurance program, and supporting technologies are designed to address whether a company's processes are relevant, effective, and resilient against today's most prevalent attack techniques. HITRUST's assurance process enables real-time quality management over every assessment and issued report.

As AI reshapes the threat landscape, including how organizations operate and manage risk, the principles outlined in this Trust Report will become even more critical. Using adaptable threat intelligence, centralized quality assurance, third-party inheritance, and transparent reporting of a company's risk exposures, HITRUST continues to evolve its system of assurance to meet the demands of this rapidly changing landscape.

In an environment where trust can no longer be implied by a report or a checkbox, HITRUST remains focused on delivering assurance that stakeholders can rely on with confidence.

> **By aligning assurance with real-world threats and measurable outcomes, we believe it is possible not only to address today's Trust Crisis, but to build a more resilient and trustworthy digital future.**

Footnotes

[1]The Verizon 2025 DBIR (http://verizon.com/dbir) reported that "the percentages of breaches where a third party was involved doubled, going from 15% to 30%.", page 11

[2]See Page 22, HITRUST Breach Rate

[3]The Verizon 2025 DBIR (http://verizon.com/dbir) reported that "the percentages of breaches where a third party was involved doubled, going from 15% to 30%.", page 11

[4]https://www.weforum.org/publications/global-cybersecurity-outlook-2025/digest, page 6

[5]https://www.kroll.com/en/publications/cyber/data-breach-outlook-2025, page 4

[6]https://www.ibm.com/reports/data-breach, page 13

[7]https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jse

[8]http://verizon.com/dbir, page 11

[9]https://panorays.com/blog/third-party-cyber-risk-ciso-survey-2025

[10]https://www.weforum.org/publications/global-cybersecurity-outlook-2025/digest, page 6

[11]For a full list of Insights Report options, see https://hitrustalliance.net/mycsf-help/example-reports.

[12]A consensus-driven framework is slowed down due to widely circulated drafts with multiple rounds of public comment and a necessity for agreement on decisions across stakeholder groups, who can each have their own incentives.

[13]https://hitrustalliance.net/cyber-threat-adaptive

[14]https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025, Chapter 4.2

[15]https://kpmg.com/us/en/media/news/2024-cybersecurity-survey.html

[16]https://nypost.com/2025/06/24/tech/cyberattacks-reshape-hiring-priorities-for-tech-executives

[17]https://www.munichre.com/en/insights/cyber/global-cyber-risk-and-insurance-survey.html, page 9

[18]https://www.kroll.com/en/publications/cyber/data-breach-outlook-2025, page 4

[19]https://www.ibm.com/reports/data-breach, page 13

[20]https://www.ibm.com/reports/data-breach, page 13

[21]https://www.newswire.com/news/cisos-in-9-countries-vendor-ai-and-ehr-now-drive-most-healthcare-data-22688683

[22]https://www.ibm.com/reports/data-breach, page 12

[23]https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jse

[24]The scaling differences between r2 assessments and i1/e1 assessments are a result of different maturity levels available in the r2 assessment. The r2 assessments are typically out of 75 points since they require scoring at the Policy, Procedure and Implemented maturity levels, but have optional Measured and Managed levels which can increase an organization's maturity score. The e1 and i1 assessments are only scored at the Implemented maturity level, which is scored out of 100 points. For additional information maturity levels, see https://www.manula.com/manuals/hitrust/hitrust-assessment-handbook/1/en/topic/prisma-maturity-levels.

[25]The Verizon 2025 DBIR (http://verizon.com/dbir) reported that "the percentages of breaches where a third party was involved doubled, going from 15% to 30%.", page 11

[26] Journal of Accountancy, February 2026: https://editions.journalofaccountancy.com/publication/?i=859206&p=10&view=issueViewer

[27]HITRUST scoping criteria is defined in the assessment handbook: https://www.manula.com/manuals/hitrust/hitrust-assessment-handbook/1/en/topic/7-1-assessment-scoping