

HITRUST®

2025

TRUST REPORT

Creating an Ecosystem of Trust

Table of Contents

- Message from Leadership..... 3
- Executive Summary: Creating an Ecosystem of Trust 4
- The Ecosystem of Trust 6
- HITRUST Assessment Trends & Insights 8
 - Why Do Systems Fail?..... 9
 - The Need for Continual Improvement..... 12
 - HITRUST Assessment Insights 16
- HITRUST’s Evolving CSF Framework 19
 - Artificial Intelligence (AI) 21
 - HITRUST CSF Scoring Approach & Assessment Results..... 23
- HITRUST’s Quality Mechanisms 25
 - HITRUST Automated Assurance Intelligence Engine (AIE) & Pre-Submission Review. . . 26
 - HITRUST Post-Submission Assessment Review 27
 - Report Quality Process..... 28
 - Escalated QA Process..... 29
 - External Assessor Program 30
 - Continuous Quality Monitoring 31
- HITRUST Roadmap 32
 - HITRUST Continuous Assurance 33
 - HITRUST CSF Version 12 (CSF v12) 34
 - Additional Insights Reporting & AI Assurance Support..... 34
 - Assessor Performance Reporting 35
- Closing Remarks..... 36

Message from Leadership

I am pleased to share the HITRUST 2025 Trust Report. When we published our first Trust Report last year, our goal was to provide insights into the Rely-ability of a HITRUST Certification. Rely-ability is a term coined by HITRUST to help relying parties understand the key elements that are necessary for them to have trust in the results of an information assurance assessment. Relying parties — be it a customer, Board of directors, insurance underwriter, or regulators — rely on the results of an information assurance assessment to make informed decisions. We believe transparency is essential to establishing and maintaining trust in an assurance solution. HITRUST remains committed to continually iterating our processes and the basis of relevance and reliability that our system is built upon to ensure our results remain trustworthy — even as threats and regulatory expectations are continually evolving across the geographies and industries of the organizations we serve.

This year, we are expanding coverage of the HITRUST Trust Report and diving deeper into the data supporting the efficacy of the HITRUST approach. One key piece of data is our breach rate, where we continue to see improvement in the effective risk mitigation of HITRUST-certified environments with **99.41%** of our customers' certified environments not reporting a data-related security breach. In the 2025 Trust Report we have included details on the approach ensuring our HITRUST CSF framework enables relevant assessments, the proactive steps we take to continually improve the framework while also detailing how our quality mechanisms continue to evolve.

There have been many developments in information compliance and security over the prior year. Information security programs are undergoing an evolution, with new business and technology solutions incorporating AI triggering changes amid increasing scrutiny from regulators, customers, and other relying parties. AI-enabled business processes have complicated companies' threat surfaces and risk management programs. In 2024, we were excited to introduce two new AI assurance mechanisms: the AI Security Certification and the AI Risk Management Assessment. We believe both products will be beneficial for organizations seeking to mitigate risks and gain assurances around the emergence of AI. Our AI Security Certification allows those companies deploying AI models to gain and provide assurances around the security of their AI platform, while the AI Risk Management Assessment provides insights around a comprehensive set of risks for companies who use, develop, or deploy AI. We intend to include the related efficacy of our AI assessments in next year's HITRUST Trust Report.

In 2025, we will start advancing our assurance model toward Continuous Assurance. This multiyear initiative will ultimately ensure consistent and continual compliance with information protection standards and policies. Our Continuous Assurance approach will combine data from multiple sources, leverage automation to highlight potential high-risk anomalies, and facilitate ongoing risk management and decision-making.

We are excited to provide you with our second-annual Trust Report. We have learned through years of research, observations, and iteration that these approaches are effective. We are publishing the evidence to better inform those who rely on our assurance assessments and certifications — including an invitation to seek out comparable information from any assurance instrument you rely upon.

Relying party and assessed entity support has been instrumental in shaping our organization, and our collective efforts continue to drive meaningful progress in effectively and practically managing information risk and compliance.

Sincerely,



Daniel Nutkis
Founder and Chief Executive Officer
HITRUST


Executive Summary:

Creating an Ecosystem of Trust


Trust acts as a cornerstone for effective communication, collaboration, and mutual respect in business interactions. When companies can trust each other, they create an environment that instills confidence and security across various stakeholders. This sense of confidence and security is essential for organizations to foster collaboration, facilitate smooth business transactions, build strong relationships, and achieve shared goals.

When it comes to information security, an organization can build trust by demonstrating it has implemented necessary robust security infrastructure and processes. The organization can prove this through various assurance mechanisms, such as HITRUST. However, for an organization to truly provide the necessary confidence to its stakeholders, the assurance mechanism must be both *reliable* and *relevant* for its purposes.


HITRUST has iterated processes over time to create an ecosystem of trust for all stakeholders through *relevant* assessments and *reliable* results. In the 2025 Trust Report, we have documented these processes (with supporting data) to assist stakeholders with not only understanding why a HITRUST certification can be trusted but providing a proven approach for performing effective foundational security.




CREATING AN ECOSYSTEM OF TRUST
WITH POWERFUL NETWORK EFFECTS



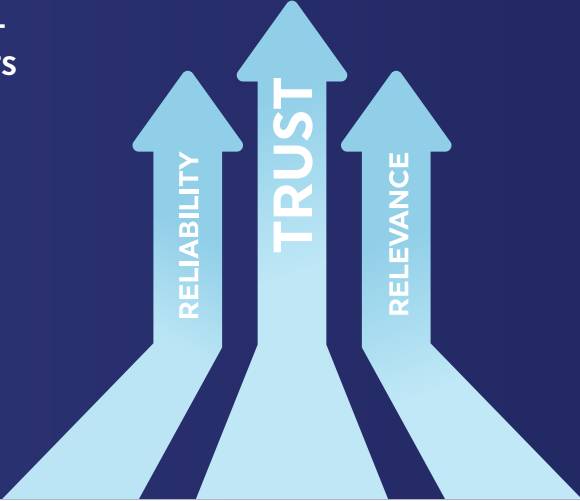
Assessed Entity: Organizations seeking to certify their security and risk management posture.



Assessors: Organizations authorized by HITRUST to help companies assess, achieve, and maintain compliance with the HITRUST framework.



Relying Party: Organizations leveraging HITRUST to secure supply chains and manage third-party risk.



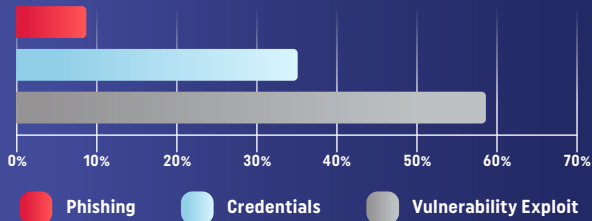
Ultimately when deploying a risk mitigation solution, organizations want to know it is working. We have collected and reviewed the necessary data to be able to demonstrate that our process works. Other assurance providers have, so far, been unable to quantify the validity of their mechanisms in this way. We believe the security outcomes in this report prove that HITRUST assurances are working, such as:

- 99.41% of HITRUST-certified environments did not report a security breach to HITRUST in 2024.
- Organizations with HITRUST certifications improve their security posture year over year. Repeat HITRUST customers in 2024 had 32% fewer requirements that needed remediation (corrective actions) in their next r2 assessment and 54% fewer corrective actions in their next i1 assessment.
- The most common path attackers use to initiate a breach is account compromise. 30% of the requirements in the e1, which is often viewed as the entry point to our portfolio, mitigate threats occurring through this attack vector.

99.41%

of HITRUST-certified environments did not report a security breach to HITRUST in 2024.

Security Breach Types Reported to HITRUST



Security Breach Type	Percentage
Phishing	~10%
Credentials	~35%
Vulnerability Exploit	~58%

54%

HITRUST Repeat Customers had 54% fewer corrective actions in their i1 assessments.

HITRUST

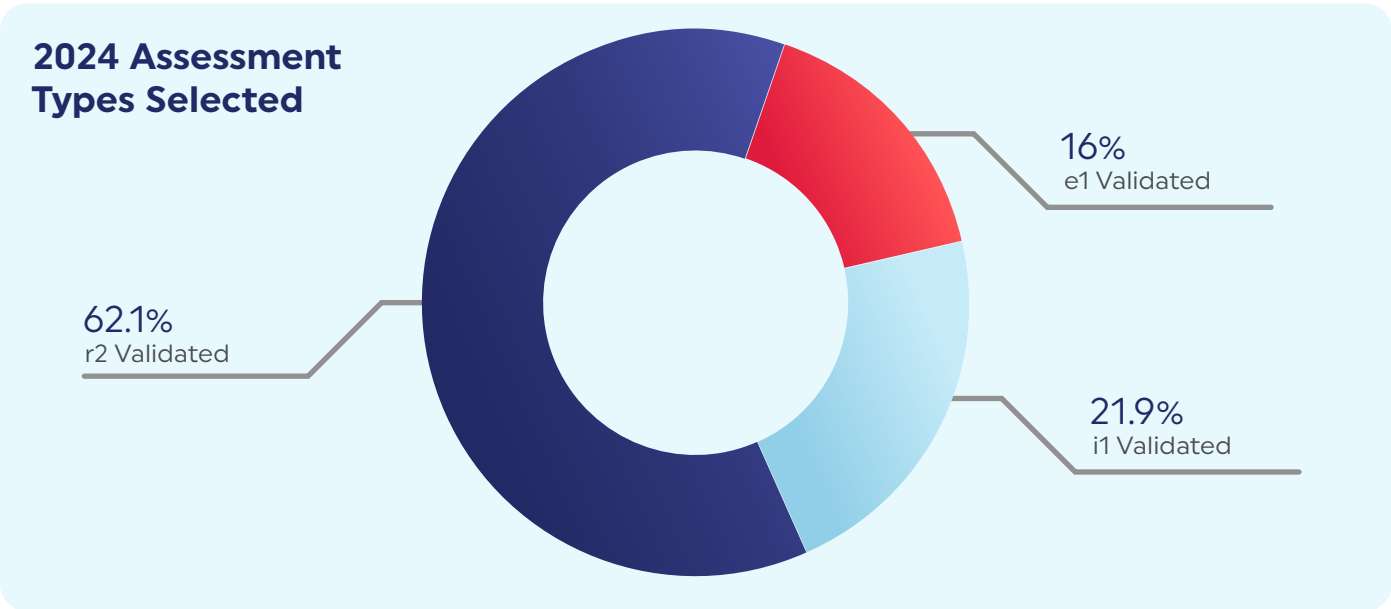
The HITRUST 2025 Trust Report

4

In addition to demonstrating our security outcomes, we have committed to key processes ensuring our certifications remain *relevant* and *reliable*. These assurance processes have also been highlighted throughout this report, including:

- In 2024 HITRUST introduced two new assurance products for risk associated with Artificial Intelligence (AI). These products support those organizations attempting to navigate the novel security threats of this emerging technology and fulfilling HITRUST's commitment to remaining continually relevant in a constantly changing threat environment.
- HITRUST performs over 250 automated quality checks on all HITRUST assessments and reports using its Assurance Intelligence Engine (AIE).
- All HITRUST assessments continue to go through our centralized quality assurance process consisting of six separate layers to ensure integrity of the assessment results, including a layer of governance providing oversight of our assurance mechanism.
- HITRUST's Inheritance functionality enables organizations to seamlessly incorporate controls of their service providers into their own HITRUST assessments. In 2024, over two-thirds (69%) of r2 validated assessments, 67% of i1 validated assessments, and 60% of e1 validated assessments utilized inheritance.

At HITRUST we believe we are building an assurance mechanism that organizations and their stakeholders can trust. In a constantly shifting threat landscape and regulatory environment, our objective is to continue providing the assurances organizations need to support their information compliance and security programs.



CSF version 11.4 addresses

100% OF THREATS

able to be mitigated in MITRE ATT&CK

For Assessments Utilizing Inheritance, External Assessors Spent

14% FEWER HOURS on r2 assessments

23.4% FEWER HOURS on i1 assessments

9.1% FEWER HOURS on e1 assessments

THE ECOSYSTEM OF TRUST



Organizations offer assurances to stakeholders to demonstrate they are taking the necessary steps to responsibly manage and protect their information. These assurances are provided to both internal stakeholders, such as internal audit teams, executive management, and corporate boards, and external stakeholders, including regulators, business partners, customers, and other third parties. The foundation of these assurances lies in the ability to rely on the quality and accuracy of the information presented by the provider of those assurances.

But what do we mean when we use the word "assurance"? The definition of assurance is "something that inspires or tends to inspire confidence¹." Assurance therefore more precisely defines what is expected to achieve *trust*. When an organization receives an assurance report, the expectation is that they must be able to rely upon and ultimately *trust* that document. But how do you know the report can be trusted?

To be able to *trust* an assurance report, the outcome must be *reliable* and *relevant*. Each organization should be asking important questions to providers of those assurance reports to validate this reliability and relevancy, such as:

- What was the assessment process and scoring approach?
- How did the assessment address the appropriate and necessary security threats relevant for the organization?
- How are the assessment and reporting processes independent to avoid conflicts of interest?
- What quality assurance processes were used to ensure the assessment was conducted faithfully and results reported truthfully?

It is dangerous to assume that all assurance approaches are created equal. Assurance outcomes are foundational to an organization's risk management and risk mitigation processes. If those assurances are wrong, an organization may end up making the wrong decisions for their information protection program.

Some assurance providers give too much flexibility in their approach where organizations may not be taking the necessary steps. Other assurance providers deliver a belt-and-suspenders approach that is unachievable for any small to midsize company. A properly designed assurance approach will provide an organization with the necessary flexibility, appropriate granularity, and the correct and relevant security requirements that it needs to manage its current risk landscape.

Organizations must critically assess the assurance approaches currently in place within their organizations to determine its relevancy. Does it address the risks of the organization, balancing the needs of the business with those risks? HITRUST has developed a *relevant* approach in the MyCSF framework through:

- Cyber Threat Adaptability
- Risk Assessment Tailoring
- Assessment Type Options
- Authoritative Source Mappings

For an assurance approach to be reliable, it must go through a quality assurance process prior to an organization receiving the final result. HITRUST has developed a reliable approach through the six essential principles of *Accuracy*, *Consistency*, *Scalability*, *Transparency*, *Integrity*, and *Efficiency*. In the 2024 Trust Report, we previously highlighted each of these six principles and how we have designed our assurance program to provide appropriate and transparent levels of assurance that organizations can trust. In this year's Trust Report, we'll continue to review key metrics highlighting how HITRUST achieves those principles in addition to new metrics highlighting trends we're seeing in HITRUST assessments.

¹Merriam-Webster Dictionary (<https://www.merriam-webster.com/dictionary/assurance>)



ACCURACY • CONSISTENCY • SCALABILITY • TRANSPARENCY • INTEGRITY • EFFICIENCY

QUALITY ASSURANCE PROGRAM

Assurance Intelligence Engine Review

HITRUST Pre and Post Submission Reviews

Escalated QA Process

Report Quality Process

External Assessor Program

Continuous Quality Monitoring

HITRUST CSF FRAMEWORK

Authoritative Source Mapping

Cyber Threat Adaptive (CTA)

Risk-Scalable

HITRUST ASSESSMENT METHODOLOGY

Maturity Model & Scoring Rubric

HITRUST Assessment Workflow

HITRUST Assessment Handbook

After choosing and adopting an assurance approach, it is necessary for organizations to know that it is working to improve their information security posture. If the assurance process is not continually evolving and adapting to the threat environment, it runs the risk of becoming exposed to new threats. **HITRUST knows its assurance approach works because we are continually reviewing the data that supports it and improving the processes based on the results.**

We will review the following in this year's Trust Report:

- HITRUST Assessment Trends & Insights
- HITRUST's Evolving CSF Framework: How the CSF framework contributes to a relevant assessment
- HITRUST's Quality Mechanisms: How the HITRUST assurance process contributes to a reliable assessment
- HITRUST Roadmap: Future enhancements providing new information security assurance options for organizations

Assessment Types

Throughout this report, HITRUST will refer to its various assessment types: the e1, i1, and r2.

- The HITRUST e1 assessment is a one-year certification which provides entry-level assurance focused on the most critical cybersecurity controls and demonstrates that essential cybersecurity hygiene is in place.
- The HITRUST i1 assessment is a one-year certification which addresses cybersecurity leading practices and a broader range of active cyber threats than the e1 assessment while providing a moderate level of assurance.
- 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.

HITRUST ASSESSMENT TRENDS & INSIGHTS

Every completed assessment must be submitted to HITRUST for review prior to HITRUST issuing the organization's report and certification letter. In addition to ensuring consistency, transparency, and integrity through a centralized QA process, this centralized submission process provides a repository of assessment data. The unique ability for HITRUST to have this data allows us to identify assessment insights and trends. We'll review this data to get a better understanding in a few areas:

- **Why Do Systems Fail?**
- **The Need for Continuous Improvement**
- **HITRUST Assessment Insights**

WHY DO SYSTEMS FAIL?

Having a centralized assessment submission process allows HITRUST to maintain records of all HITRUST-certified organizations and require those organizations to maintain their level of security throughout the life of their certification. HITRUST maintains three key processes to identify whether a HITRUST-certified organization experienced a security breach:

- All HITRUST-certified organizations are contractually obligated to notify us when they have identified a security breach in their HITRUST-certified environment. These commitments are reviewed and renewed with each subsequent certification.
- External Assessors must examine with each organization whether they experienced a security breach upon the one-year anniversary of an r2 assessment (during the interim assessment). HITRUST evaluates any potential breaches on each interim assessment submission.
- HITRUST proactively monitors publicly available sources to identify potentially unreported breaches from HITRUST-certified organizations.

Through this centralized assessment submission process, HITRUST is the only assurance provider able to collect and review security breach data to quantify how well our assurance process is working. We calculate our security breach rate based on the rate of reported breaches to HITRUST-issued certifications. **We noted 99.41% of HITRUST-certified environments did not report a security breach in 2024.** This represents an increase in environments without a reported security breach when compared to the 99.36% rate noted in last year's Trust Report.

There is no centralized repository to identify all security breaches (in the U.S. or globally), but surveys, publicly available data, and required regulatory reporting all provide insights into the number of companies experiencing data breaches:

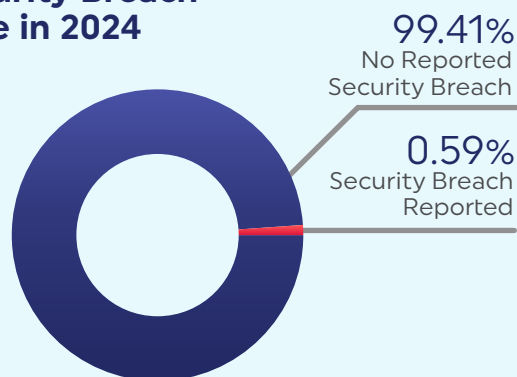
- Munich RE's *Global Cyber Risk and Insurance Survey 2024* interviewed 7,500 participants from 15 countries across various sectors and found 47% of the interviewed companies had been affected by a cybersecurity breach, with 87% indicating they were not prepared for a cyberattack.
- Vanson Bourne, a UK-based tech market intelligence organization, interviewed 1,000 IT decision-makers from IT security in March 2023 and found that 60% of respondents experienced authentication-related breaches over the prior 12 months.
- Government agencies across the United States received 6,908 notifications of data breaches in 2024 (per the Data Breach Chronology database by Privacy Rights Clearinghouse). The Data Breach Chronology database draws from 15 U.S. government agencies that maintain public records of data breach notifications.
- 706 data breaches involving protected health information and affecting 500 or more individuals were reported to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) in 2024.

Based on this data, along with other generally reported breach findings, we can infer the security breach rate for HITRUST-certified organizations is likely lower than those without a HITRUST certification.

Did You Know?

Many other assurance providers do not have a centralized assurance process. These other assurance providers specify the framework to be followed, while outsourcing their quality assurance and report issuance processes. In addition to limiting their ability to manage the assurances others are providing on its behalf, those providers do not have the data to know whether their assurance process is actually working.

Security Breach Rate in 2024

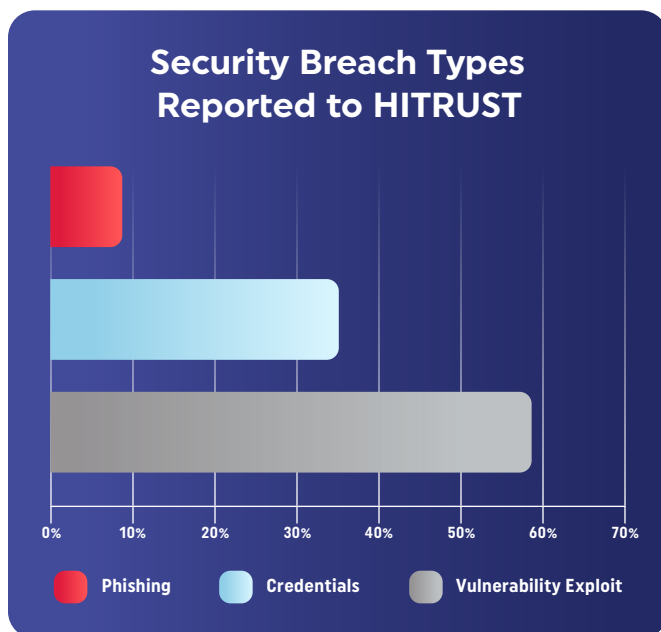


Healthcare Industry Breaches

While the healthcare industry has always had a high share of security breaches due to the sensitive nature of the industry, it has been hit particularly hard in 2023 and 2024. While the number of breaches reported to OCR has not dramatically increased, there has been a much larger increase in the size of the security breaches. According to data published on OCR's breach portal:

- Five of the 10 largest security breaches have occurred in the past two years.
- In 2023, over 133 million individual records were exposed, an increase of 156% from 2022.
- In 2024, over 185 million individual records were exposed.

Looking further into our breach figures, we identified the most common breach type for HITRUST-certified organizations over the prior three years was a result of system vulnerabilities, **with over 50% of security breaches reported to HITRUST resulting from vulnerability exploits (including both externally and internally developed software).***



Vulnerability Exploit

Involves taking advantage of a security flaw in software or hardware.

Credentials

Involves the information used to authenticate and authorize a user or identity, most commonly usernames and passwords.

Phishing

Involves a victim receiving a message (typically via email or phone) to trick them into revealing sensitive personal information or downloading malware.

This data aligns with results from the Verizon 2024 Data Breach Investigations Report (Verizon 2024 DBIR), where exploits involving vulnerabilities, which includes zero-day software vulnerabilities, have almost tripled from the prior year:

Our ways-in analysis witnessed a substantial growth of attacks involving the exploitation of vulnerabilities as the critical path to initiate a breach when compared to previous years. It almost tripled (180% increase) from last year, which will come as no surprise to anyone who has been following the effect of MOVEit and similar zero-day vulnerabilities. These attacks were primarily leveraged by ransomware and other extortion-related threat actors. As one might imagine, the main vector for those initial entry points was Web applications.

– Verizon 2024 Data Breach Investigations Report

*We note there may be overlap where a security breach may have multiple causes (e.g., phishing leading to a vulnerability exploit). In these instances we recorded the primary cause which initiated the security breach.

The Verizon 2024 DBIR also identified the category of Credentials (representing the compromise of account credentials) as the largest reported path to initiate a data breach (most often through the use of compromised accounts on a web application). Notably, this was the second-highest reported path for HITRUST-reported security breaches. In the e1 assessment which addresses the security essentials for every organization, 30% of the HITRUST requirements are related to the HITRUST Access Control and Password Management domains to protect against those attack vectors.

Security Breach

HITRUST defines a security breach as any security incident in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, used, disclosed, or accessed in an unauthorized fashion and/or by an individual or organization unauthorized to do so and compromises the privacy or security of the data.

The third most common security breach type reported to HITRUST (and second-highest path to initiate a breach in the Verizon 2024 DBIR) was related to successful phishing attempts. As noted in the Verizon 2024 DBIR:

The overall reporting rate of phishing has been growing over the past few years. In security awareness exercise data contributed by our partners during 2023, 20% of users reported phishing in simulation engagements, and 11% of the users who clicked the email also reported.

– Verizon 2024 Data Breach Investigations Report

While Verizon notes that only 20% of company users are reporting phishing attempts in those simulations, HITRUST includes this as a requirement for a company's phishing training. Starting with the HITRUST e1 assessment and included in all subsequent assessment types, organizations must perform dedicated phishing awareness trainings. Within these phishing trainings, HITRUST requires that organizations train employees to recognize and report potential phishing attempts to improve their awareness.

As threats evolve over time and attackers become more sophisticated, it is not possible to be fully protected from a security breach. However, organizations can reduce their exposure considerably by implementing and maintaining appropriate levels of threat coverage. Although the threat coverage (and assurance) levels differ across HITRUST assessment types, HITRUST continually performs threat analysis to ensure each assessment type addresses a broad range of the most common attack tactics. **We believe this threat analysis process within HITRUST is one of the key reasons why HITRUST-certified organizations are better protected from security breaches.**

THE NEED FOR CONTINUOUS IMPROVEMENT

Security needs for an organization are constantly evolving as security breach patterns and trends change over time. As an example, the Verizon 2014 DBIR indicated that System Intrusion, including ransomware, was one of the leading breach causes over the prior three years. However, in 2020 it wasn't even in the top three.

System Intrusion continues to be the top pattern from a breach perspective (as opposed to incidents, where DoS attacks are still king). Both the Social Engineering and Miscellaneous Errors patterns have risen appreciably, particularly the latter, since last year. Conversely, the Basic Web Application Attacks pattern has fallen dramatically from its place in the 2023 DBIR.

– Verizon 2024 Data Breach Investigations Report

As a result of these constantly evolving threats, HITRUST assessments are cyber threat-adaptive to ensure organizations perform relevant assessments that address the latest critical threats such as ransomware.

HITRUST consumes threat intelligence data from a leading threat intelligence provider, maps those threats to the MITRE ATT&CK framework, and utilizes that data to identify the necessary requirements for a HITRUST assessment. As cyber threats evolve over time, the HITRUST CSF is reviewed and enhanced to ensure new and emerging threats are mitigated.

However, it's not enough for only HITRUST to adapt. Information security managers must maintain an understanding of the current threats they are facing and consistently improve their security posture. Our market-level intelligence shows that most HITRUST-certified organizations are improving their security posture through the remediation of identified deficiencies in their assessments.

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.

The remediation of CAPs contributes to the continual improvement of a HITRUST certification holder's security posture. As HITRUST-certified customers remediate identified CAPs over time, we would expect to see reduced CAPs as those organizations recertify. **We see this reduction on a year-over-year basis overall with 7% fewer HITRUST assessments having CAPs in 2024 than 2023 across all assessment types.** When broken down by assessment type, 26.5% of the e1 assessments had at least one CAP, while 88.5% of the i1 assessments reported one or more CAPs.

Interim Assessment

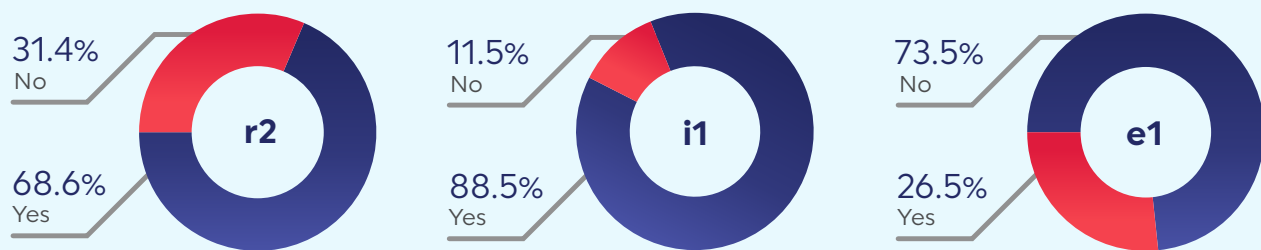
All organizations who achieve an r2 certification must complete an interim assessment by the one-year anniversary of its certification to maintain its r2 certification for the full two-year cycle. Criteria for completing the interim assessment includes:

- Successful validation of a sample of HITRUST requirements
- No degradation of the control environment (e.g., through security breaches or significant changes)
- Sufficient progress remediating CAPs

Validated Assessments with Corrective Action Plans (CAPs)



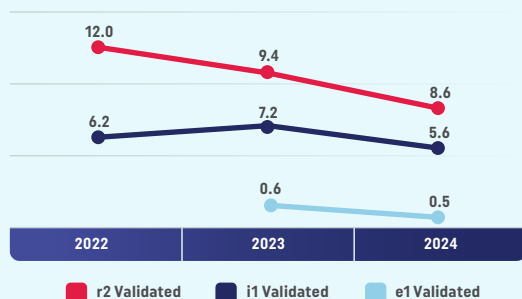
2024 Validated Assessments with CAPs by Assessment Type



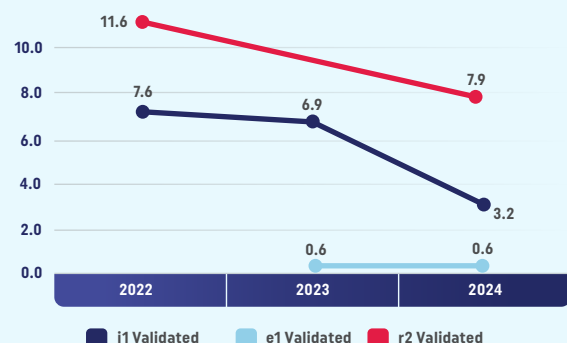
When we dive deeper to identify the average number of CAPs within each assessment, we identified that (as expected) r2 assessments average the highest number of CAPs while e1 assessments average the least number of CAPs. On a year-over-year basis, we noted a reduction in the average number of CAPs in r2 and i1 assessments between 2023 and 2024.

The HITRUST i1 and e1 assessments do not require organizations to demonstrate sufficient remediation of CAPs to HITRUST since interim assessments are not performed on one-year assessments. Interestingly, we still observe improvement on the number of CAPs in both assessment types when we review the average number of CAPs in assessments where the organization was a HITRUST customer in both 2023 and 2024. **In fact, we observed significant improvement in the security posture of repeat HITRUST customers who had 32% fewer CAPs on average in their next r2 assessment and 54% fewer CAPs on average in their next i1 assessment.**

Average Number of CAPs per Assessment by Assessment Type



Average Number of CAPs for HITRUST Returning Customers



We identified the top 10 HITRUST requirements which required remediation through CAPs in 2024. The list is based on the rate of occurrence for a CAP when the corresponding HITRUST requirement was included in the organization's assessment (ranked from highest occurrence rate). Although the CAPs are mostly disparate across the HITRUST assessment domains, we noted that three of the top 10 HITRUST requirements were in the Access Control domain. This further aligns with the challenges organizations face with protecting themselves from account compromises, as previously noted based on the results of the Verizon 2024 DBIR.

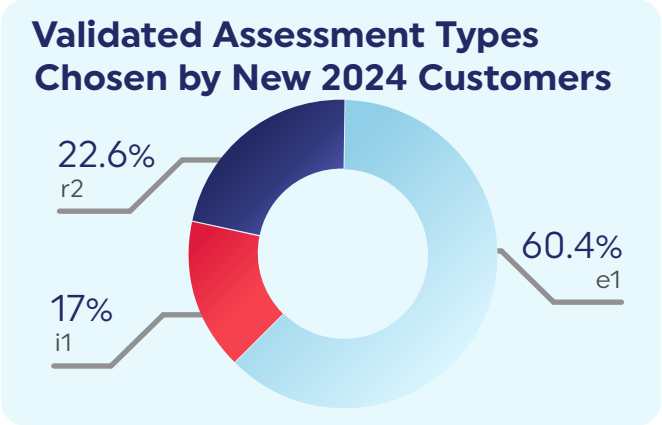
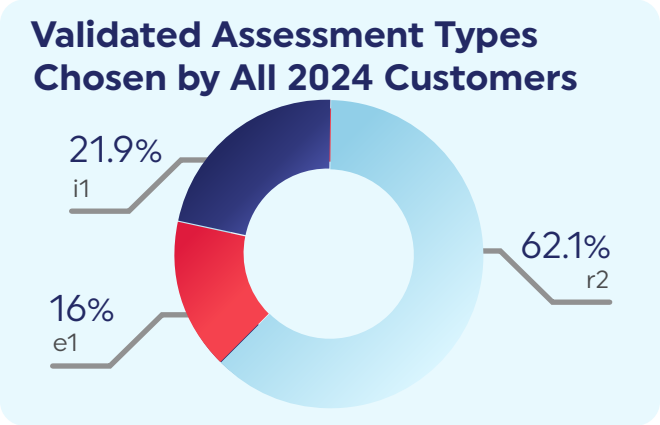
Ranking	HITRUST Domain	HITRUST Requirement ID	HITRUST Requirement Description
1	Third-Party Assurance	1411.09f1System.1	The organization ensures a periodic review of service-level agreements (SLAs) is <ul style="list-style-type: none"> 1. conducted at least annually, and 2. compared against the monitoring records.
2	Network Protection	0835.09n10Organizational.1	The ability of the network service provider to manage agreed services in a secure way is <ul style="list-style-type: none"> 1. determined and 2. regularly monitored. The right to audit <ul style="list-style-type: none"> 3. is agreed by management for each network service provider. The security arrangements necessary for particular network services' <ul style="list-style-type: none"> 4. security features, 5. service levels, and 6. management requirements are identified and documented.
3	Audit Logging & Monitoring	12101.09ab1System.2	The organization specifies <ul style="list-style-type: none"> 1. how often audit logs are reviewed, 2. how the reviews are documented, and 3. the specific roles and responsibilities of the personnel conducting the reviews, 4. including the professional certifications or other qualifications required.
4	Vulnerability Management	0706.10b1System.2	The organization develops applications based on secure coding guidelines to prevent <ul style="list-style-type: none"> 1. common coding vulnerabilities in software development processes 2. injection flaws, particularly SQL injection (validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.) 3. buffer overflow (validate buffer boundaries and truncate input strings) 4. insecure cryptographic storage (prevent cryptographic flaws) 5. insecure communications (properly encrypt all authenticated and sensitive communications) 6. improper error handling (do not leak information via error messages) 7. broken authentication/sessions (prevent unauthorized individuals from compromising legitimate account credentials, keys, or session tokens that would otherwise enable an intruder to assume the identity of an authorized user) 8. cross-site scripting (XSS), e.g., validate all parameters before inclusion, utilize context-sensitive escaping, etc. 9. improper access control, such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access functions (e.g., properly authenticate users and sanitize input, and do not expose internal object references to users) 10. cross-site request forgery (CSRF), e.g., do not reply on authorization credentials and tokens automatically submitted by browsers; and 11. any other input-validation vulnerability listed in the OWASP Top 10.
5	Access Control	11.01p1System.5	A policy applicable to the organization's information systems addressing account lockout after consecutive unsuccessful login attempts is <ul style="list-style-type: none"> 1. documented and 2. enforced through technical control.

Ranking	HITRUST Domain	HITRUST Requirement ID	HITRUST Requirement Description
6	Access Control	11143.02i10Organizational.3	The organization ensures <ol style="list-style-type: none"> 1. logical and 2. physical access authorizations to systems and equipment are reviewed, updated, or revoked when there is any change in 3. responsibility or 4. employment.
7	Access Control	11.01e1System.2	The organization reviews all <ol style="list-style-type: none"> 1. accounts (including user, privileged, system, shared, and seeded accounts) and 2. privileges (e.g., user-to-role assignments, user-to-object assignments) periodically (annually at a minimum).
8	Risk Management	1739.05d10Organizational.3	Management <ol style="list-style-type: none"> 1. formally authorizes (approves) new information assets and facilities for processing (use) before commencing operations and periodically reviews and updates authorizations (approvals) at a frequency defined by the organization—but no less than three years.
9	Business Continuity & Disaster Recovery	1632.12a10Organizational.1	The organization <ol style="list-style-type: none"> 1. identifies all the assets involved in critical business processes 2. considers the purchase of suitable insurance which may form part of the overall business continuity process, as well as being part of operational risk management 3. ensures the safety of personnel and the protection of information assets and organizational property; and 4. formulates and documents business continuity plans addressing information security requirements in line with the agreed business continuity strategy.
10	Data Protection & Privacy	19249.06b10Organizational.2	The organization <ol style="list-style-type: none"> 1. establishes restrictions on the use of open source software. Open source software used by the organization is <ol style="list-style-type: none"> 2. legally licensed, 3. authorized, and 4. adheres to the organization's secure configuration policy.

HITRUST ASSESSMENT INSIGHTS

In January 2023, the HITRUST assessment portfolio was expanded with the introduction of the e1 assessment. The introduction of this assessment type was made to create additional options for organizations wanting to select the right assessment approach based on their needs and risk exposure. We recognized at the time that the market was missing a mechanism for organizations to demonstrate assurance around the basic security essentials.

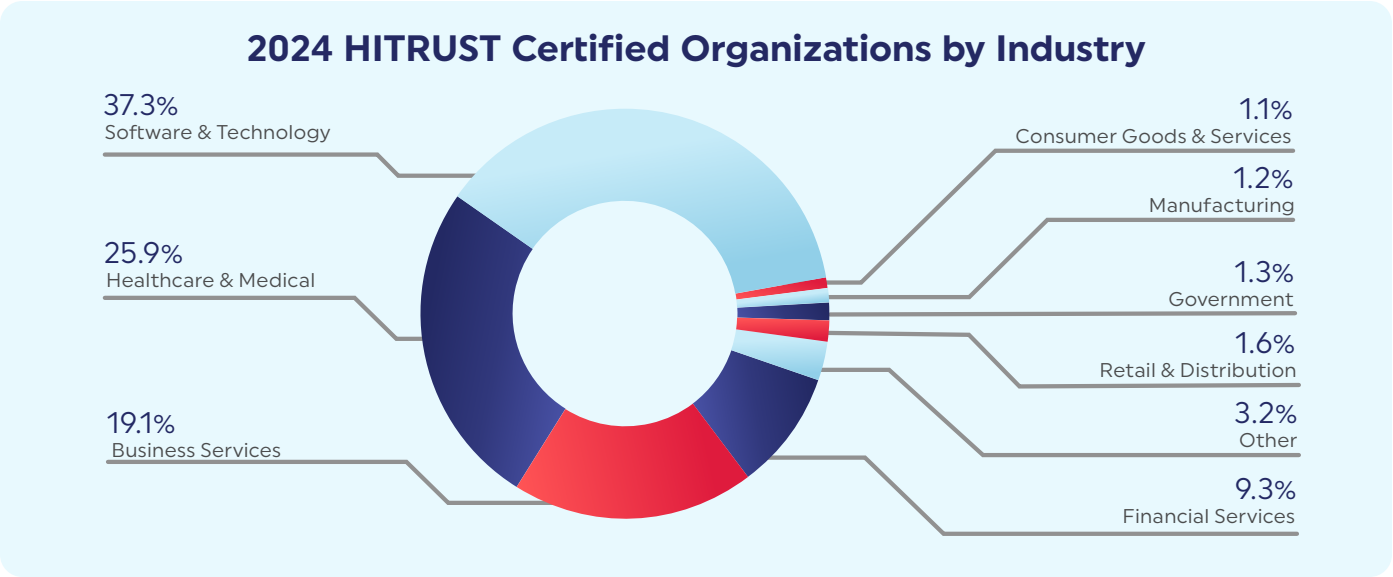
In 2023, we noted the majority (47.6%) of new customers chose to start their HITRUST journey with the HITRUST e1 assessment, further demonstrating there was a need for this type of assurance mechanism. **We saw this trend continue in 2024 with over 60% of new customers opting for the e1.** At the same time, HITRUST noted the majority of customers continued to opt for the highest level of assurance with over 62% performing the HITRUST r2 assessment.



Assessment Industry Performance

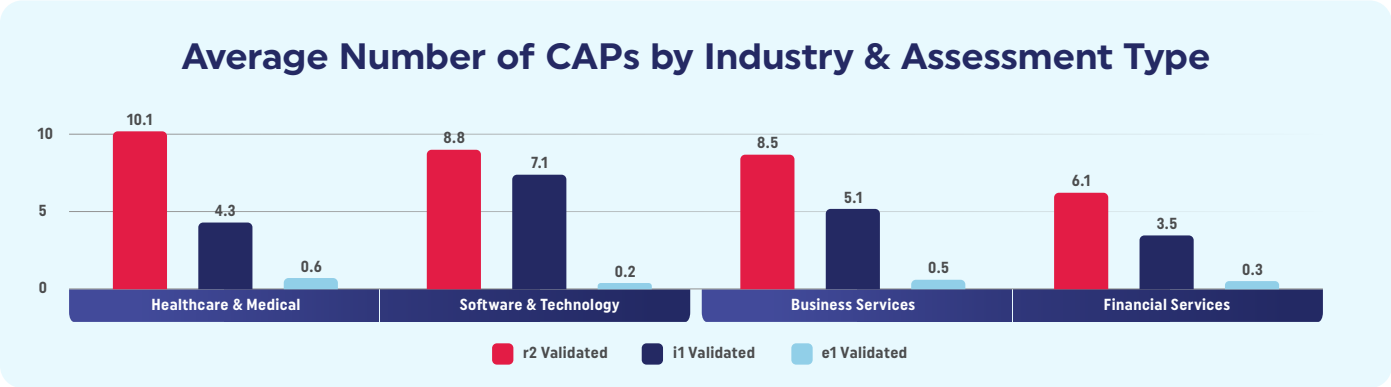
Since we were founded in 2007, HITRUST has championed programs that safeguard sensitive information and manage information risk for global organizations across all industries and throughout the third-party supply chain. HITRUST has continually broadened the ability for organizations of all sizes and industries to utilize and benefit from a HITRUST assessment.

The top four industry sectors that obtained a HITRUST certification in 2024 represented over 90% of HITRUST assessment volume. These industries included **software & technology, healthcare & medical, business services, and financial services.**

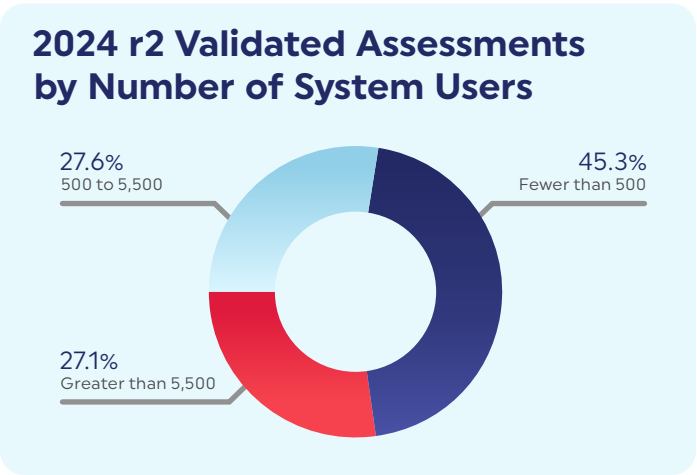


Each of these industry sectors reflects a different risk profile and assessment needs. Across the top four HITRUST-certified industries, we noted the following in their 2024 assessments:

- Financial Services had the lowest average number of CAPs across both r2 and i1 assessments.
- Healthcare & Medical had the highest average number of CAPs per r2 assessment.
- Software & Technology had the highest average number of CAPs per i1 assessment.

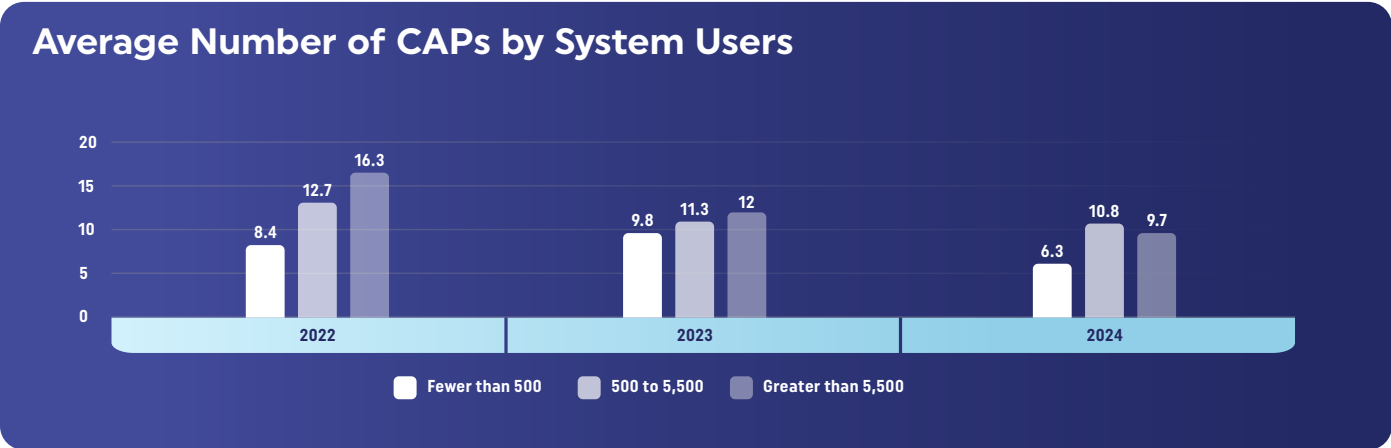


Within a HITRUST r2 assessment, one of the questions that tailors the risk of an assessment is the number of users who could access the in-scope platform. In 2024, we identified that around 45% of the assessments had less than 500 users, while the other two options (between 500 and 5,500 users, and greater than 5,500 users) were each selected in approximately 27% of the assessments.



In reviewing whether the size of the in-scope platform (based on number of users) impacted the average number of CAPs, we identified for HITRUST r2 assessments:

- Smaller platforms (less than 500 users) had the fewest average number of CAPs, both in 2024 and on a year-over-year basis since 2022.
- The largest platforms (greater than 5,500 users) have reduced their average number of CAPs by 40% since 2022.
- In 2024, the midsize platforms (between 500 and 5,500 users) had the highest average number of CAPs in an r2 assessment.

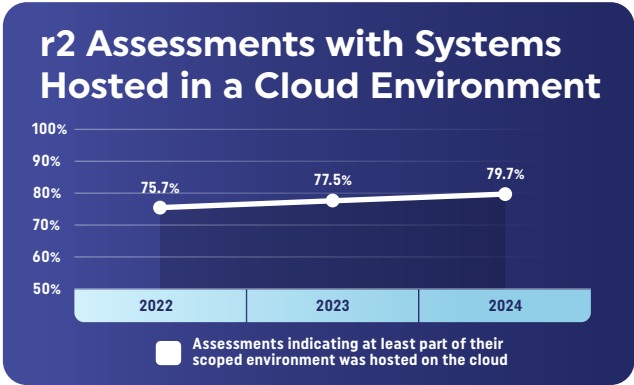


We also reviewed data around customers utilizing Cloud Service Providers. In 2024, almost 80% of HITRUST-certified assessments maintained at least part of their scoped environment in the cloud. This represents a 4% increase from 2022.

Inheritance

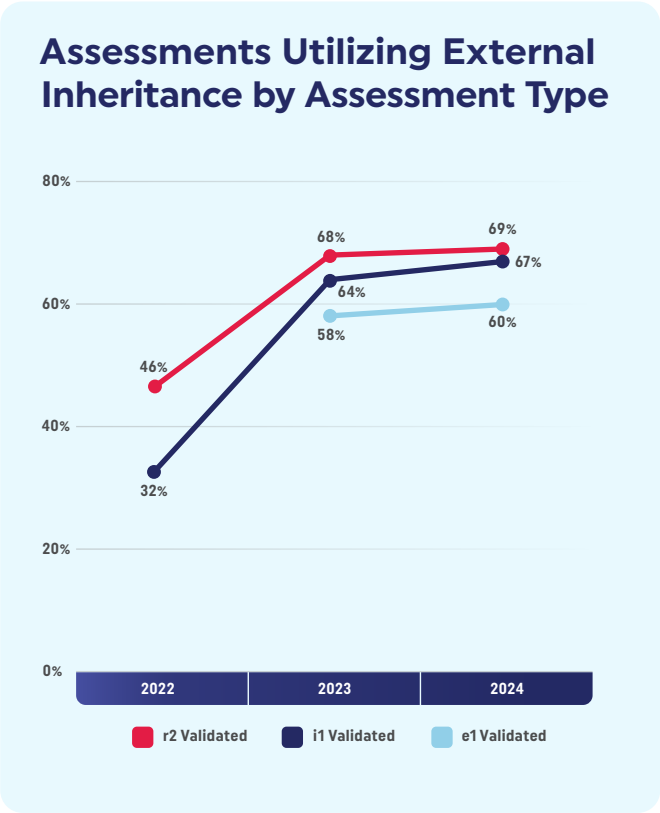
In today's IT landscape, most platforms rely on service providers for various components, creating additional layers of risk that traditional assurance approaches often overlook. HITRUST addresses this gap through its **Inheritance** functionality, which enables organizations to seamlessly incorporate the validated controls of their service providers into their own HITRUST assessments.

HITRUST stands out as a superior assurance mechanism because it accounts for the complexities of the underlying technology stack and the opportunity to increase security efficiency by inheriting security from service providers. This approach ensures that risk is assessed holistically across the entire technology stack, reducing duplicative testing, increasing efficiency for small and midsize companies, and providing the most robust and efficient path to certification. By facilitating collaboration and transparency between organizations and their service providers, HITRUST delivers a level of assurance that is uniquely tailored to the interconnected nature of modern IT systems.



Did You Know?

Although many other assurance providers do not require service providers to be considered as part of an organization's security assessment, HITRUST requires them to be assessed in every r2 assessment. Since the r2 represents the highest level of assurance, it is necessary to consider the risks posed by service providers. **According to the Verizon 2024 DBIR, 15% of security breaches were due to a third party, a 68% increase from the previous year.**



In 2024, we continued to see a year-over-year increase in the use of inheritance in HITRUST assessments with over two-thirds (69%) of r2 validated assessments utilizing External Inheritance, while 67% of i1 validated assessments and 60% of e1 validated assessments used External Inheritance.

Organizations utilizing inheritance see both lower certification costs and faster times to achieve HITRUST certification. Based on External Assessor reported hours in 2024, we noted the following inheritance efficiencies.

On average, External Assessors spent:

- 14% FEWER HOURS** on r2 assessments which used inheritance
- 23.4% FEWER HOURS** on i1 assessments which used inheritance
- 9.1% FEWER HOURS** on e1 assessments which used inheritance

HITRUST'S EVOLVING CSF FRAMEWORK

HITRUST assessments work because the CSF framework provides the structure, transparency, guidance, and cross-references to authoritative sources that organizations globally need to be certain of their data protection compliance. Within the CSF framework, HITRUST maintains the requirements that an organization needs to achieve certification.

However, for a framework to maintain relevance it must contain the information protection requirements that organizations need to protect their environment against the current threat landscape. This is why HITRUST assessments are cyber threat-adaptive, to allow changes as the threat landscape evolves.

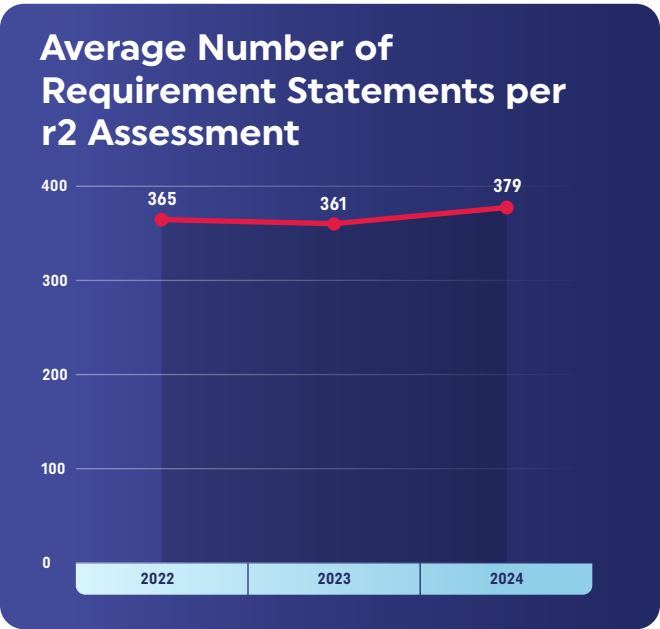
CSF FRAMEWORK

HITRUST uses the MITRE ATT&CK framework to assist with identifying the appropriate requirements for inclusion in the CSF. The MITRE framework details the various methods or tactics that adversaries operate during a cyber attack. MITRE has then identified various mitigations to prevent or significantly hinder an attacker from successfully executing that tactic. **The HITRUST e1 assessment addresses 62% of these MITRE mitigations, while the HITRUST i1 and r2 assessments address 100% of the MITRE mitigations.**

While the e1 and i1 assessments include a fixed number of HITRUST requirements (44 and 182 respectively), the r2 is a risk-based and tailorable assessment where the number of requirements depends on the results of a HITRUST risk analysis. The risk analysis is performed to ensure the r2 provides the highest level of assurance for situations with greater risk exposure due to data volumes, regulatory compliance, or other risk factors. **In 2024 HITRUST noted that an r2 validated assessment averaged approximately 379 requirements**, which reflects a slight increase from the average of 361 requirements in 2023.

Did You Know?

HITRUST is the only assurance provider who maintains cyber threat-adaptive assessments. Other assurance providers often leave organizations to figure out which requirements will address the applicable threats for their environment. HITRUST has already done the work and provides scalable and tailorable assessments for all organizations.



The HITRUST CSF framework includes requirements which are based on various types of authoritative sources to incorporate the necessary requirements in each organization's assessment. **In December 2024, HITRUST introduced CSF version 11.4 which now incorporates 60 authoritative sources, an increase of 36% over the last year.** Utilizing such a large universe of potential controls is what makes the HITRUST CSF suitable for organizations of all types and sizes, regardless of industry. With each additional version of the CSF, HITRUST continues to expand this body of authoritative sources, which demonstrates its commitment to maintaining a comprehensive control framework.

Several of the sources incorporated into the latest versions of the CSF allow HITRUST to remain relevant to the advent of Artificial Intelligence through certification and Insights Reports related to Artificial Intelligence, as we'll explore next.

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

When an organization performs a HITRUST r2 assessment, it is able to select Compliance factors related to these sources which incorporates that source's HITRUST requirements into its assessment.

ARTIFICIAL INTELLIGENCE (AI)

Using any new technology brings about new inherent risks, and this is especially true in the case of AI. While AI presents opportunities, it also introduces unique risks and compliance challenges that demand attention. Excitement about AI, like all new systems, has the potential to relegate critical security and assurance considerations to afterthoughts. Managing the security risks of AI systems is critical, as failing to do so can have severe consequences.

The deployment of an AI model imposes novel security threats while exacerbating others, requiring additional cybersecurity measures that are not comprehensively addressed by most risk frameworks and approaches. Compared to traditional software, AI-specific security risks include the following:

- Issues in the data used to train AI models can bring about unwanted outcomes, as intentional or unintentional changes to AI training data have the potential to fundamentally alter AI system performance.
- AI models and their associated configurations are a high-value target to attackers who are discovering new and stealthy approaches to breach AI systems.
- Modern AI deployments rely on third-party service providers to an even greater degree, making supply chain risks such as software and data supply chain poisoning an increased threat and solutions such as inheritance and shared responsibility essential to AI security outcomes.
- AI systems may require more frequent maintenance due to rapid changes in the threat landscape and data, model, or concept drift.

IN 2024 WE INTRODUCED TWO NEW METHODS FOR ORGANIZATIONS TO GAIN ASSURANCE OVER AI:

**HITRUST AI SECURITY
CERTIFICATION**

**HITRUST AI RISK
MANAGEMENT ASSESSMENT**

HITRUST AI Security Certification (ai1 & ai2)

The HITRUST AI Security Certification, ai1 (when combined with an e1 or i1 assessment) and ai2 (when combined with an r2 assessment), is designed to deliver an AI Security Assessment and accompanying certification for deployed AI systems.

The HITRUST AI Security Assessment includes:

- 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.
- Clearly specified and understandable security requirements which can be included in any HITRUST e1, i1, or r2 assessment by selecting the Security for AI Systems compliance factor in MyCSF.
- The same reliability as other HITRUST certifications since it goes through the same rigorous quality assurance processes as all other HITRUST assessments.

Did You Know?

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

The introduction of AI is one of many strides that HITRUST expects to take in broadening the relevance of a HITRUST assessment for organizations. HITRUST anticipates introducing several additional Insights Report types for organizations who are looking toward expanding their information protection assurance in 2025 and beyond.

As of version 11.4.0 of the HITRUST CSF, 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). Upon completion of an ai1 or ai2 assessment which achieves the certification criteria (for both the underlying HITRUST validated assessment and the ai1 or ai2 assessment), HITRUST will issue an AI Security Certification Report.

HITRUST AI Risk Management Assessment

While the AI Security Certification focuses on mitigating the AI security threats that make up the cybersecurity risk that accompanies the deployment of AI within an organization, cybersecurity risk is only one of many risks discussed in AI Risk Management frameworks like the NIST AI RMF and ISO/IEC 23894:2023. AI risks that are peers to cybersecurity include those dealing with AI ethics (such as fairness and avoidance of detrimental bias), AI privacy (such as consent for using data to train AI models), and AI safety (i.e., ensuring the AI system does not harm individuals). HITRUST's AI Risk Management Assessment and Insights Report is designed to help organizations report on the larger AI Risk Management problem.

The HITRUST AI Risk Management Assessment is a comprehensive solution designed for organizations using, developing, and/or deploying AI. **It offers detailed AI Risk Management insights based on 51 relevant and practical risk management controls.** The HITRUST requirements provide clear, prescriptive definitions of policies, procedures, and implementations that can be measured and evaluated. These requirements go through identical quality assurance procedures as all HITRUST assessments to provide reliable results.

In order to provide relevant results, the assessments are harmonized with ISO/IEC 23894:2023 and NIST RMF, providing insights on their performance in both ISO and NIST terms which allows organizations to prioritize their next steps.

HITRUST CSF SCORING APPROACH & ASSESSMENT RESULTS

Assessment results in an assurance report are expected to accurately reflect the security state of the organization's environment. As a result, assurance providers must have mechanisms in place to facilitate the accurate evaluation and scoring of implemented controls.

To help assessors score control maturity in a consistent, accurate, and repeatable way, HITRUST developed a scoring rubric to be used in scoring evaluations. **100% of validated assessments submitted to HITRUST in 2024 utilized the HITRUST scoring rubric to evaluate the organization's control maturity.**

When an entity has not fully implemented a HITRUST requirement within the scope of its assessment, or when deficiencies in the operation of those controls are identified, the control maturity scores are lowered based upon the HITRUST scoring rubric. 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. In the table below, HITRUST identified the most difficult domains for organizations to achieve maturity based on the lowest scores by assessment type. For the r2 and e1, the most challenging domains continue to be the same in 2023 and 2024. **The fact that organizations struggle with Password Management and Access Control is consistent with the Verizon 2024 DBIR results, where Credentials continues to be the most common path for attackers to initiate a breach.**

Did You Know?

HITRUST provides the only assessment report that articulates control maturity using a PRISMA-based control maturity and scoring model. This provides a level of accuracy not achievable by traditional assessment approaches. For an r2 assessment, the status of an organization's information security *policies, procedures, and controls implementation* must be assessed as part of the maturity model. **This provides a higher level of assurance because it is based on direct rather than circumstantial evidence** and therefore is more indicative of the actual level of protection the organization provides, making it the most accurate method of measuring the performance of an organization's controls.

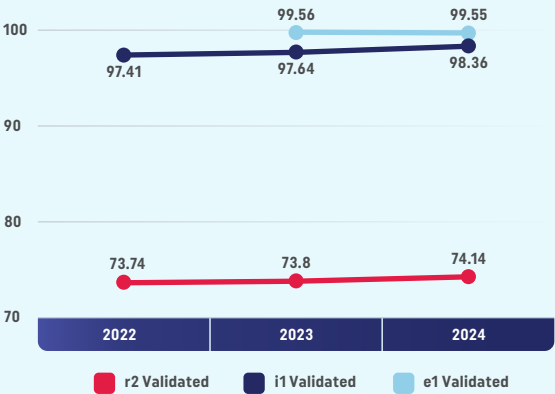
Lowest Scoring Domain by Validated Assessment Type

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

In addition to Vulnerability Management being the lowest scoring domain for the i1, it was a close second place in lowest scoring domain for the r2. **This trend towards lowered scores in that domain is, again, consistent with the 180% growth of the exploitation of vulnerabilities as a critical path for attackers to initiate a breach, as noted in the Verizon 2024 DBIR.**

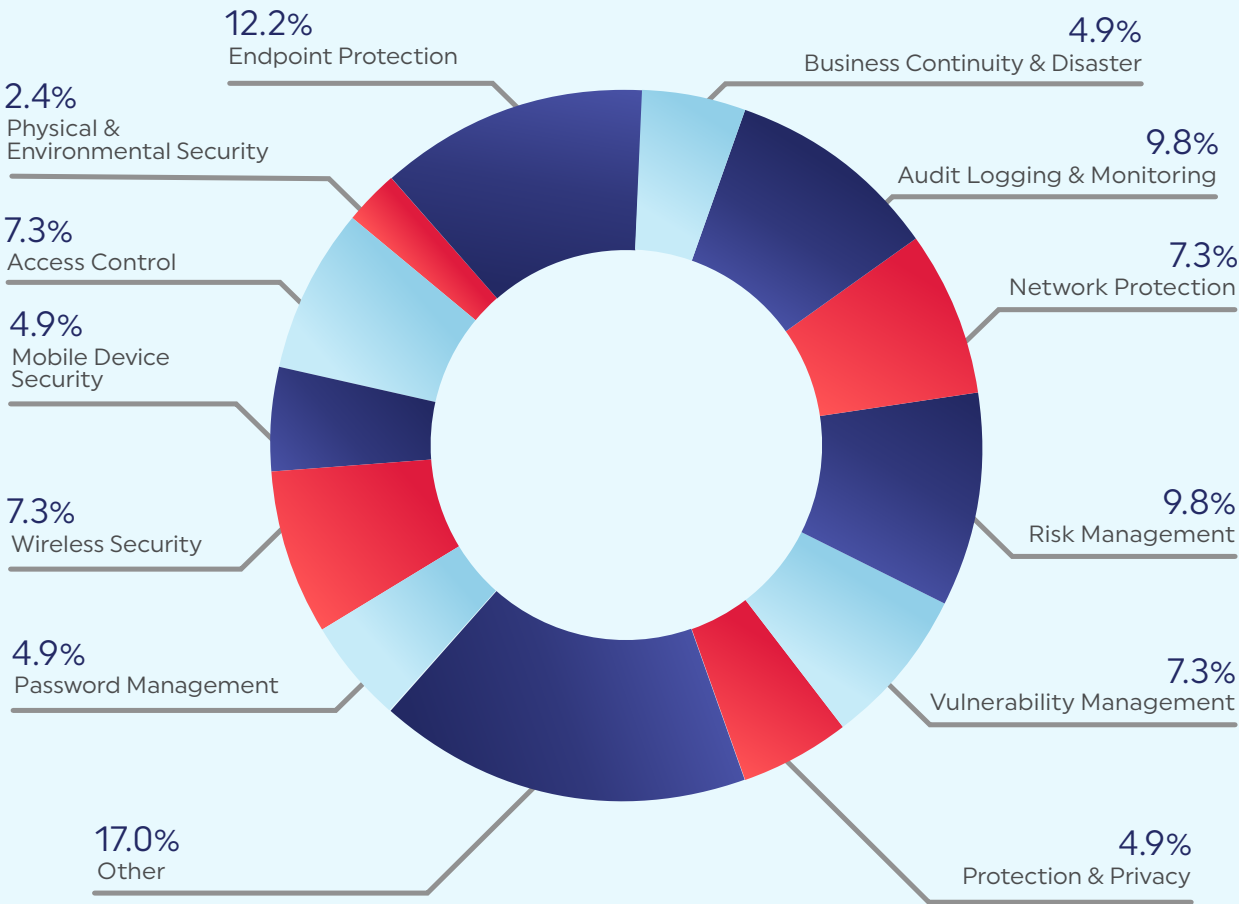
When reviewing the assessment maturity scores on a year-over-year basis, we noted an increase in the overall average scores for the i1 and r2 assessments from 2022 to 2024. Between 2022 and 2024, the i1 scores improved by .95 points (1%) and the r2 improved by .40 points (.5%). The e1 assessment maintained a similar score in 2023 and 2024 with a difference of only .01 points. This aligns with the improvements noted earlier on average number of CAPs in an assessment. Over time, HITRUST customers appear to improve their information security posture.

Average Assessment Scores by Assessment Type



Less than 1% of assessments submitted to HITRUST in 2024 failed to achieve certification. This is not surprising since most customers do not submit assessments which do not achieve the certification threshold. **For those assessments submitted to HITRUST which failed certification, the most common domain causing them to fail certification was Endpoint Protection.** This domain includes requirements for protecting those devices which can access the in-scope environment, including user laptops, desktops, and mobile devices. These are common targets for attackers attempting a remote system intrusion but can also represent a weakness as a stolen asset.

Percent of Failing Domains for Non-Certified Assessments



HITRUST'S QUALITY MECHANISMS

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

The HITRUST Assurance Program has several layers, including:

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

HITRUST AUTOMATED ASSURANCE INTELLIGENCE ENGINE (AIE) & PRE-SUBMISSION REVIEW

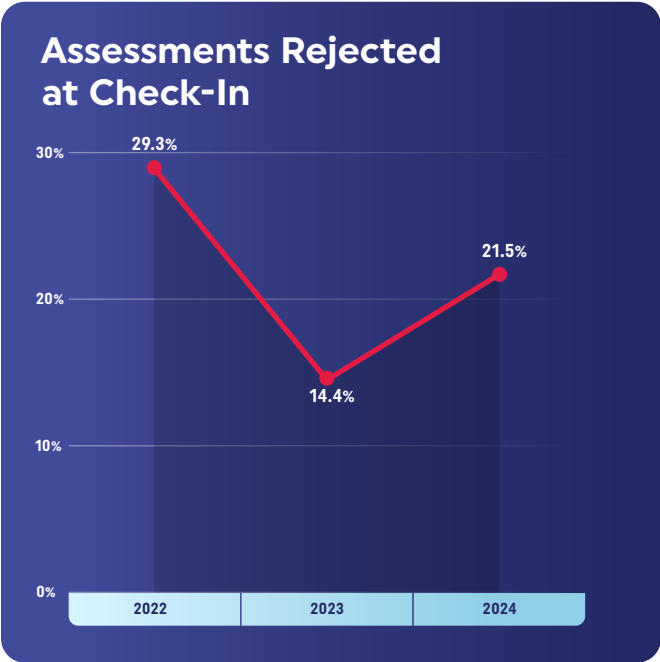
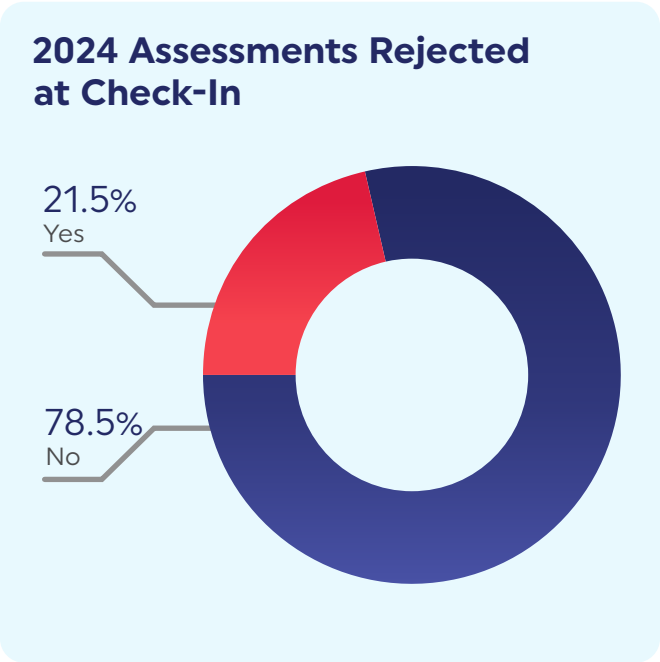
The HITRUST AIE is an automated process within MyCSF which identifies potential quality issues during an assessment and upon assessment submission. The AIE proactively identifies potential issues by performing a real-time analysis against thousands of data points across the body of documentation for an assessment. During an assessment in the MyCSF platform, the AIE provides detailed descriptions for potential quality issues, the triggering data point(s), and recommended remedial actions.

Upon submission, the assessment undergoes over 190 automated quality checks to identify and address assessment errors and omissions. 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 2024, the AIE returned 21.5% of submissions back to the External Assessor for additional review of quality issues, representing an increase of over 7% from 2023.**

Did You Know?

Most assurance providers do not have a centralized QA process to ensure consistent quality, accuracy, and integrity of reports issued based on their frameworks. They often rely on third-party firms to perform the work and issue the final reports without reviewing the results themselves. Unfortunately, this results in inconsistency in approach and final results across the various firms, along with potential conflict of interests.

We believe that having this centralized QA process with multiple manual and automated layers of oversight is the most important step to ensure the reliability of a certification report.

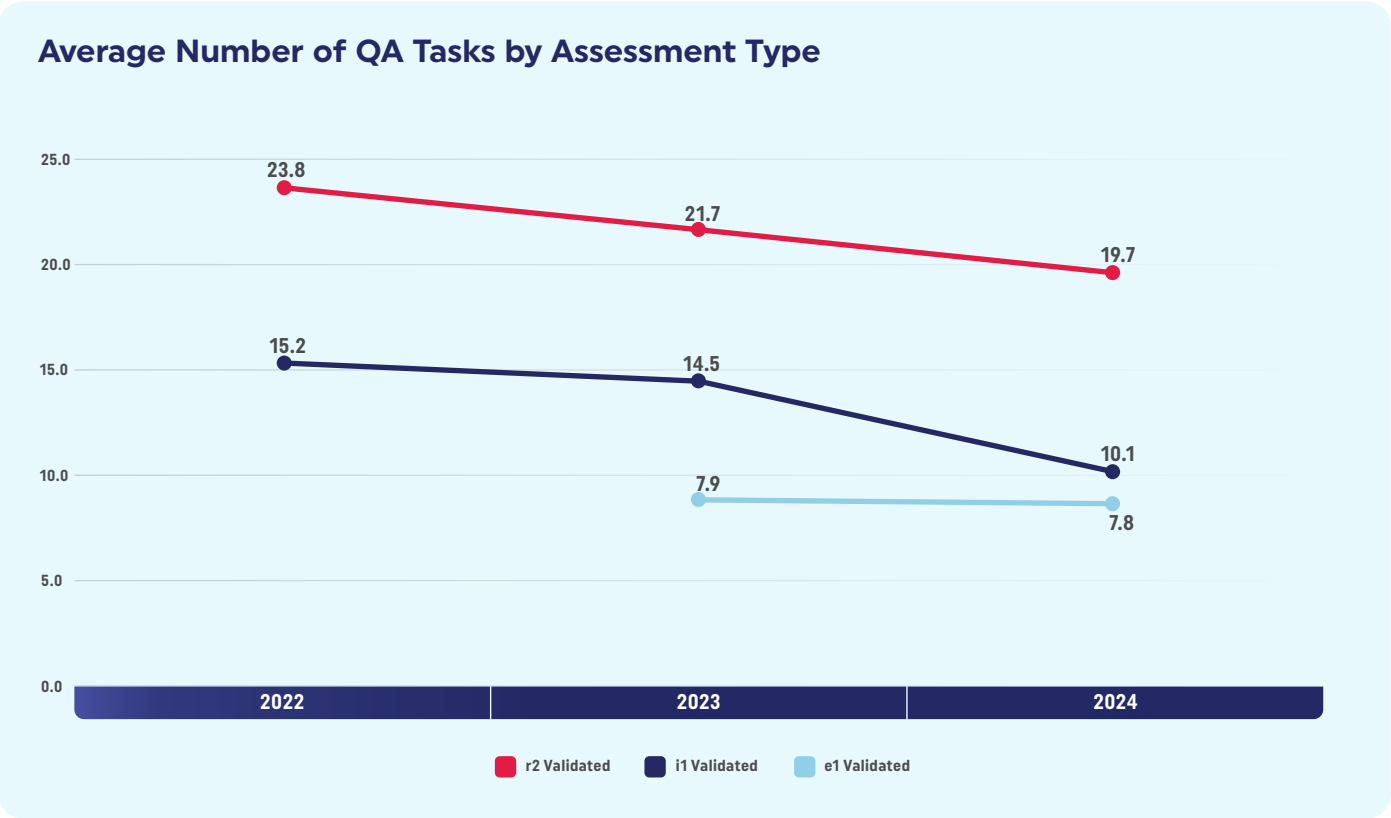


HITRUST POST-SUBMISSION ASSESSMENT REVIEW



Each validated assessment must undergo a detailed quality assurance (QA) review after it has been submitted to HITRUST. The QA review uses a risk-based approach to determine the required level of review for each assessment. The appropriate QA risk level for each assessment is identified through a set of analytics that HITRUST runs on the assessment upon submission. After determining the QA risk level, a HITRUST QA Analyst will perform the QA review. During the QA review, the HITRUST QA Analyst will review each potential quality issue, ensure the assessment information meets HITRUST criteria defined in

the 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. **Overall, we saw a reduction in the average number of QA tasks on a year-over-year basis, with 23% less tasks being opened in 2024 vs. 2023.** This may indicate further maturity and understanding of the expected approach by External Assessors when performing a HITRUST assessment.

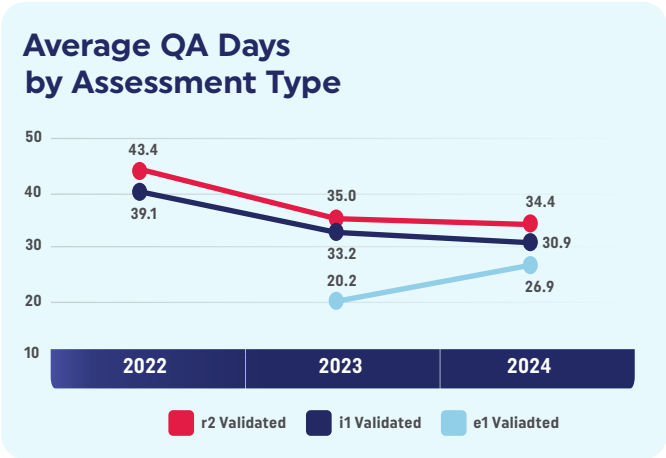


REPORT QUALITY PROCESS

Reports are initially prepared by HITRUST analysts with the assistance of the HITRUST AIE and reviewed by two levels of HITRUST management prior to issuance. The HITRUST AIE performs over 60 additional automated checks on the report to identify any potential quality issues. After the HITRUST QA Analyst prepares the draft report, it is reviewed by Assurance management and then sent to the HITRUST Quality team for a second management review. Upon approval from the HITRUST Quality team, the draft report is released in MyCSF to the organization for its review and final approval.

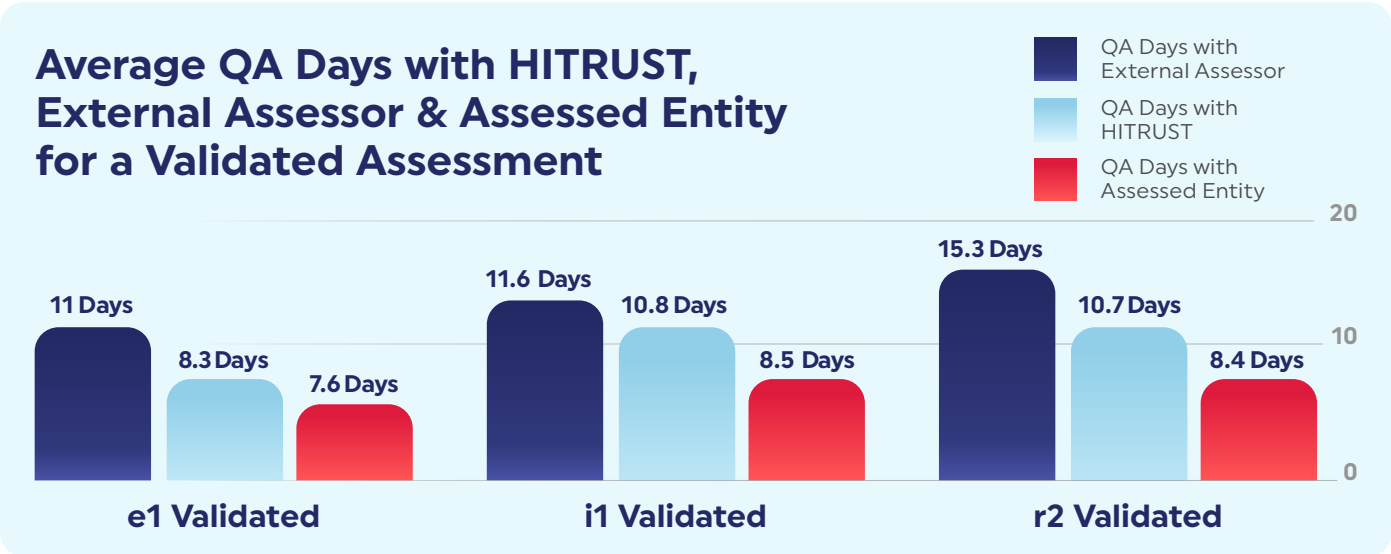
HITRUST uses an automated Reservation System within the MyCSF platform to streamline the QA-to-draft report process. The Reservation System requires organizations to schedule the start of their QA prior to submitting a HITRUST validated assessment. The Reservation System is designed to:

- 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 2023 to 2024 for an r2 and i1, but increased for an e1 assessment.

Although we saw an increase in the number of days in QA for an e1, it remains lower than Service-Level Agreement (SLA) of 30 days with HITRUST for the e1. We have also committed to an SLA of 45 days with HITRUST for the i1. If HITRUST does not meet the SLA, the organization's next i1 or e1 validated assessment report credit is complimentary. In 2024 HITRUST did not exceed this SLA threshold for any i1 or e1 assessments.



ESCALATED QA PROCESS

HITRUST maintains an Escalated QA (EQA) process for those assessments where the HITRUST QA Analyst has identified a higher volume and/or severity of concerns than typically expected. An assessment only enters Escalated QA if HITRUST believes that the nature of the concerns may be pervasive enough to affect scoring across the validated assessment.

In EQA, the HITRUST Quality team attempts to understand the procedures performed by the External Assessor during fieldwork to validate the assessment scoring. The EQA team will communicate and meet with the External Assessor at least two times to attempt to resolve HITRUST's questions and concerns. At the end of EQA, HITRUST will either return the validated assessment back to normal QA or provide options to remediate the assessment which may include lowering scores, providing additional evidence, or performing a new validated assessment. If a validated assessment re-enters EQA a second time after remediation, and the External Assessor is unable to resolve HITRUST's concerns, it will be considered a failed QA. **In 2024, no submissions failed the HITRUST QA process.**

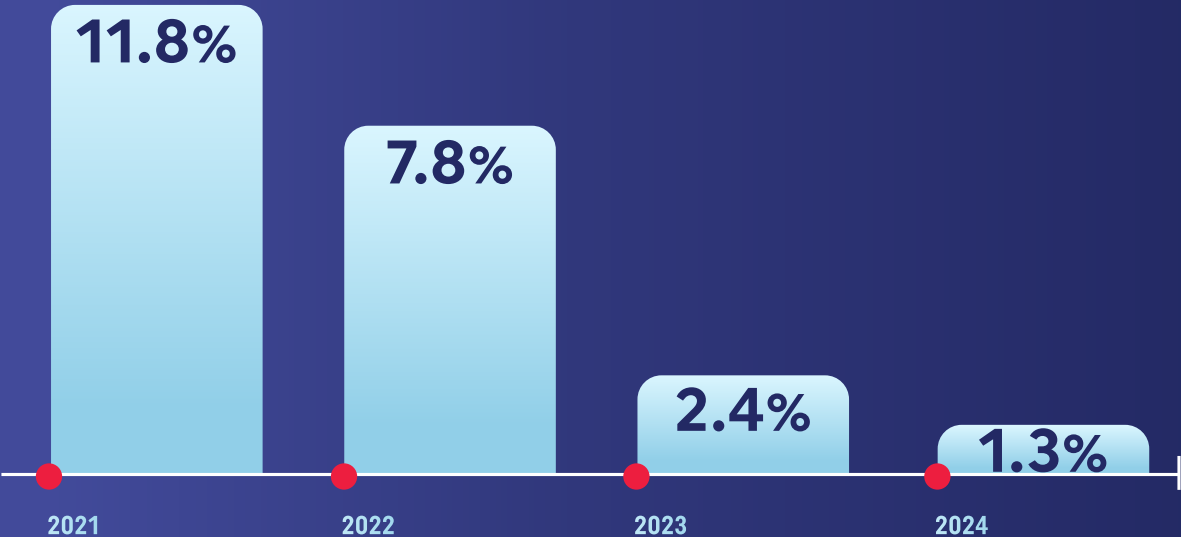
We saw another decrease in the percentage of submitted validated assessments entering Escalated QA from 2023 (2.4%) to 2024 (1.3%). This reduction can likely be attributed to the increased communication between the HITRUST Assurance and Quality teams with the External Assessor community, along with an increased understanding in the HITRUST community of our expectations through the publication of the HITRUST Assessment Handbook in October 2023.

Did You Know?

Some assurance mechanisms lack published clarity and transparency in their assessment processes. HITRUST's robust assessment approach, control maturity and scoring methodology, and related assurance requirements are clearly articulated in the publicly available HITRUST Assessment Handbook.

The HITRUST Assessment Handbook defines the requirements for those organizations assessing their information protection programs against the HITRUST CSF through a readiness or validated assessment. The HITRUST Assessment Handbook was updated to version 1.1 on December 6, 2024, with additional guidance for combined assessments and the AI Security Certification.

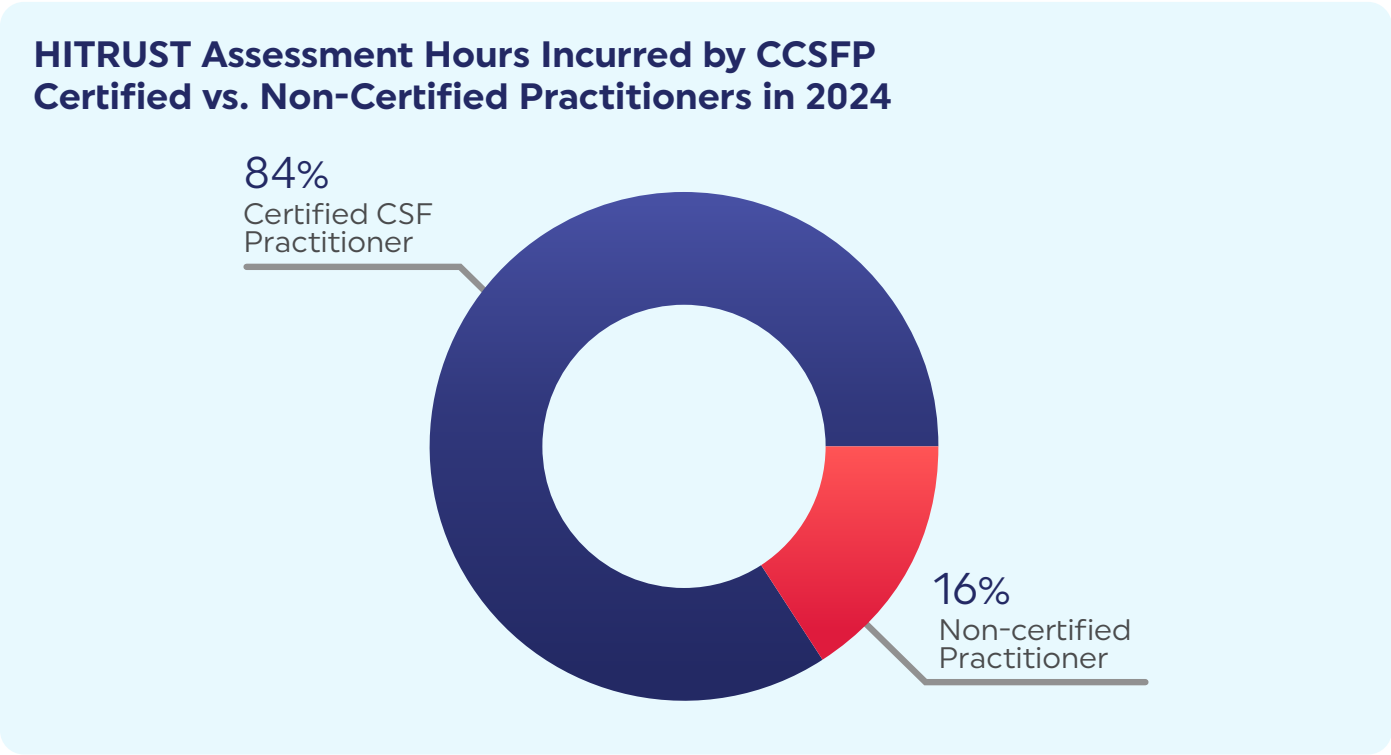
Assessments Entering Escalated QA Over Time



EXTERNAL ASSESSOR PROGRAM

All organizations must engage with a HITRUST-authorized External Assessor to perform validation procedures prior to completing and submitting a HITRUST validated assessment. HITRUST's External Assessors Program is supported by a pool of independent HITRUST Authorized External Assessor ranging from large global professional services firms to small boutique consultancies. This program has also proven itself extremely capable of supporting the wide and varied needs of industry as demand for HITRUST CSF Validated Assessment Reports has continued to grow over the past decade. **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.**

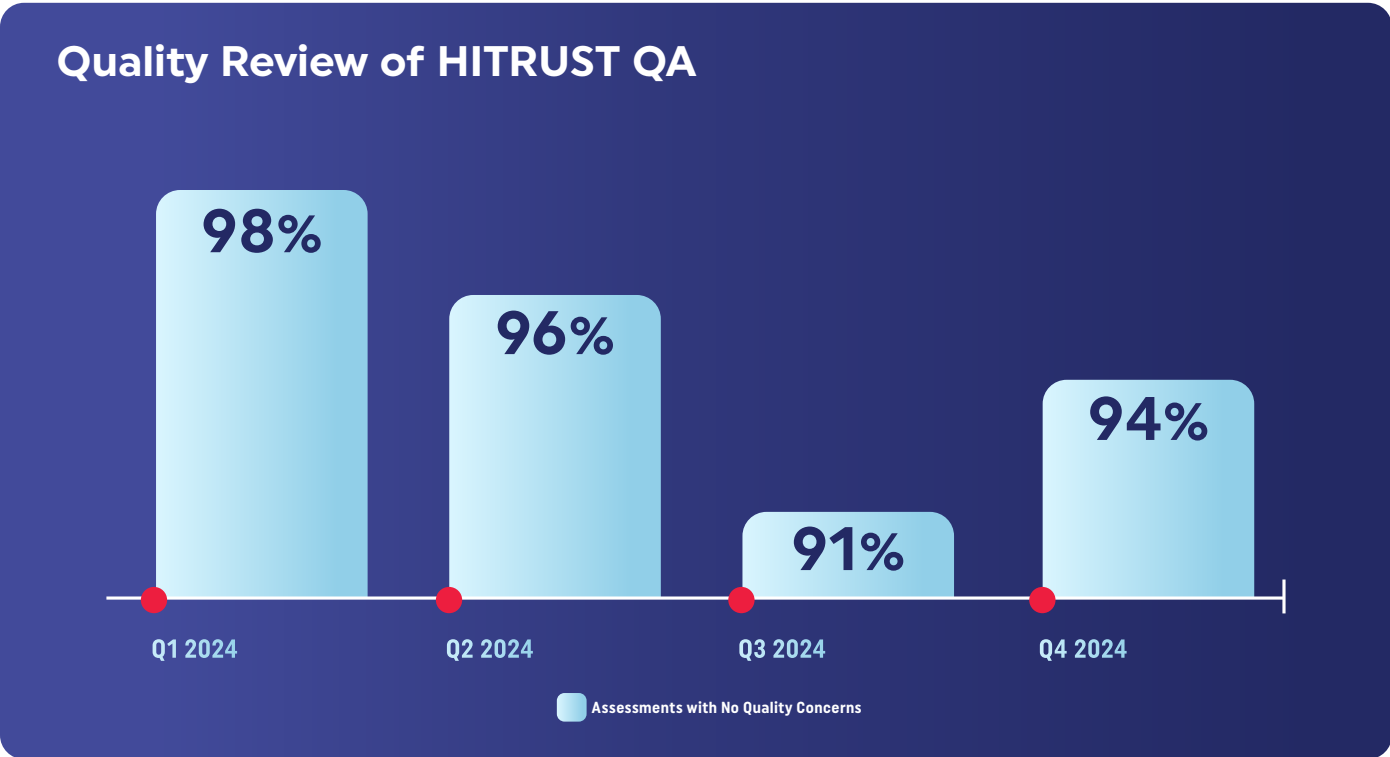
External Assessor firms within the HITRUST External Assessor Program must maintain a minimum of five practitioners with the CCSFP designation and two practitioners with the CHQP designation. For each submitted validated assessment, at least 50% of all engagement hours must be performed by practitioners with a CCSFP to ensure the team has an appropriate understanding of the HITRUST CSF and HITRUST Assurance Program methodologies and tools. Additionally, the External Assessor's quality assurance reviewer must hold both a CCSFP and CHQP designation. That reviewer may not perform other roles on the assessment (e.g., assessment testing) to help ensure the objectivity of the External Assessor's review. **In 2024, 84% of hours on each submitted validated assessment were performed by an individual with a CCSFP designation which represented an increase of 10% from 2023.**



CONTINUOUS QUALITY MONITORING

Quality performance is continuously monitored and audited by the HITRUST Quality department, with quality metrics reported quarterly to the Quality Assurance Advisory committee and HITRUST CEO. The Quality department is separate from the HITRUST Assurance department, providing increased independence.

To ensure consistency in feedback across HITRUST QA Analysts, the HITRUST Quality department reviews all HITRUST QA Analysts on a monthly basis. During its review, the HITRUST Quality team reperforms the QA Analyst's assessment review to ensure they reached the appropriate conclusion consistent with the HITRUST Assessment Handbook. This review confirms the HITRUST QA Analyst provided and closed all necessary feedback and tasks to the organization or External Assessor prior to issuing its report and/or certification. HITRUST saw consistent high quality in the QA Analyst's performance throughout 2024 as 95% of assessments reviewed had no quality concerns.



The HITRUST Quality Assurance Advisory committee was formed to provide additional oversight of the HITRUST Assurance Program. **The role of the HITRUST Quality Assurance Advisory committee is to independently review the processes HITRUST has in place to ensure quality and consistency across the entire program.** This includes reviewing metrics used by HITRUST to measure quality at every level of the process, providing feedback where changes are required, and making recommendations for process improvements when appropriate.

The HITRUST Assurance Program includes a layer of governance which provides oversight and continual quality improvements into the entire process and program. This includes:

- HITRUST QA Advisory Committee
- MyCSF Quality & Assurance Reporting
- Continuous Quality Monitoring Process

HITRUST ROADMAP



HITRUST remains committed to ever-evolving investments that continue to raise the bar for assurances for the industries and companies that we serve. In 2025 and beyond, we are pursuing several initiatives to continue building an ecosystem of trust.

HITRUST CONTINUOUS ASSURANCE

Continuous Assurance is an ongoing process that checks for drift from a secure system state, ensuring consistent compliance with security standards and policies. It combines data from multiple sources, leverages automation to highlight potential high-risk anomalies, and facilitates ongoing risk management and decision-making. Perhaps equally important is the need to ensure that security systems continue to operate to their expected maturity levels and that policies, procedures, and implementation remain aligned with documented expectations.

As organizations continue to balance the cost and complexity of security and compliance monitoring with the need to achieve and sustain security outcomes, a systematic and efficient approach for Continuous Assurance is essential. Security threats are not static, and the need to efficiently reduce evidence decay and continually ensure that security requirements remain relevant and reliable is vital given the evolving threat landscape.

In last year's Trust Report, our roadmap included two key initiatives, both of which we achieved in 2024:

- In August 2024, we announced the e1 and i1 combined assessments. These combined assessments allow customers to combine their e1 or i1 validated assessment with an eligible HITRUST Compliance factor (e.g., HIPAA, AI Risk Management). Upon successful completion of the assessment, the organization will receive an Insights Report for each added source in addition to their e1 or i1 HITRUST CSF Report.
- As noted earlier in this Trust Report, we introduced both an AI Security Certification and an AI Risk Management Assessment in 2024. We developed these offerings in collaboration with leading AI industry vendors and their adopters to secure AI technologies and tackle the unique risks and threats AI systems face.

HITRUST Continuous Assurance will enable integration with technologies that provide security control measurement and management. The result will include greater levels of assurance by minimizing evidence decay through monitoring of key assurance evidence and security telemetry on a continuous basis — all designed to detect or avoid drift in an organization's control posture.

For HITRUST, multiple existing and planned capabilities will make Continuous Assurance possible:

- **Continuous Monitoring Taxonomy Through the Next Generation HITRUST CSF:** Control requirements require different approaches to Continuous Assurance to ensure relevancy and reliability of security maturity oversight. The identification of control requirements categories suitable for Continuous Assurance will be supported in the next generation of the HITRUST CSF, rolling out in phases beginning in 2025, starting with HITRUST CSF v12.
- **Continuous Monitoring Workflow Enhancements:** The HITRUST MyCSF will contain new workflow capabilities that allow assessed entities to publish evidence updates and seek validation of evidence of continued control sustainability. Inspection and approval will vary by control category, and the system will support the relationships and workflow needed to analyze submitted evidence and confirm that it is both suitable for the control requirement and the underlying scope of the certification. Depending on the rigor and importance of different control requirements, External Assessors will be needed to examine and validate security outcomes and will be vital contributors to Continuous Assurance outcomes.
- **Automated Evidence Collection:** HITRUST's existing Automated Evidence Collection capability supports integration with assessed entities' existing technology and compliance frameworks. These services provide an important foundation by providing the baseline of evidence used for security and compliance assurance while reducing cost and complexity.

- **Continuous Outcome Inspection:** New HITRUST services will be available beginning in late 2025 that allow qualified service providers and technology suppliers to demonstrate proven fidelity, integrity, and sufficient integration capabilities to HITRUST that inform security maturity scores and prove that security requirements remain achieved through their systems. Selected, qualified, and leading cloud service providers and security technology providers will provide these services, all delivered on top of the robust and existing shared responsibility and inheritance capabilities provided by HITRUST.
- **Results Distribution System:** HITRUST's existing digital platform enables the seamless distribution and integration of assessment and certification results, corrective action plans (CAPs), and status updates — eliminating reliance on PDF reports and allowing for electronic examination of security outcomes plus analysis of individual maturity metrics, and monitoring of remediation commitments on demand and with higher fidelity.
- **Governance, Risk, and Compliance Integration:** HITRUST assessment results and assurance outcomes may now be integrated directly into supporting third-party risk management and GRC systems, ensuring faster and more accurate analysis, quicker remediation, and increased transparency, including vital third-party risk management, workflow support with improvements in efficiency, and clear and traceable documentation with HITRUST recently announcing support for ServiceNow with the HITRUST Assessment XChange for ServiceNow.

The HITRUST Continuous Assurance approach, by design, will support both systemic control monitoring through Continuous Outcome Inspection and the collection of security artifacts with validation workflows that prove conformance with required policies and procedures. Mature and complex systems will likely require a combination of automated and artifact-oriented forms of security monitoring to ensure that policies and procedures remain relevant.

HITRUST CSF VERSION 12 (CSF V12)

CSF v12 will play a key role in the journey toward providing Continuous Assurance. As part of CSF v12, HITRUST expects to include the following key features:

- Incorporation of HITRUST Cyber Threat Analysis (CTA) into MyCSF
- Review and update of the factor questions used to tailor a HITRUST r2 assessment
- Updates to align the control references to the updated factor questions and AI controls
- Restructuring of privacy based on ISO 29151
- Additional features as necessary to align with the HITRUST Continuous Assurance approach

ADDITIONAL INSIGHTS REPORTING & AI ASSURANCE SUPPORT

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 Compliance factor (e.g., HIPAA). The first Insights Report was launched in November 2023 which included the ability to provide insights into an organization's HIPAA compliance. We expanded offerings in 2024 to provide Insights Reports on AI Risk Management and PHIPA (Ontario Personal Health Information Protection Act).

In 2025, we intend to expand Insights Reporting through the addition of eligible Compliance factors. Additional Compliance factors currently expected for implementation in 2025 include Ransomware, NIST 800-171, CMMC (Cybersecurity Maturity Model Certification) Level 1, HICP (Health Industry Cybersecurity Practices), and Department of Health and Human Services' Cybersecurity Performance Goals (CPGs).

For AI assurance, we will continue providing active support for those organizations adopting the new HITRUST AI Security Certification in 2025. We will continue performing active and ongoing monitoring of emerging standards to identify any necessary iterations of the AI requirements included in the certification. Based on the dynamics of the AI market, we will also explore the need for additional AI offerings such as validated model cards or expansion into other areas of trustworthy AI (e.g., AI governance, AI safety).

ASSESSOR PERFORMANCE REPORTING

As seen throughout this Trust Report, we have been able to collect a great deal of information on assessments submitted to HITRUST. In 2025 we intend to further explore details in this data to provide valuable information to External Assessors on their performance. This information will be used to create and provide performance reports to each External Assessor. These reports are intended to:

- Drive higher quality HITRUST assessments
- Faster times for assessments to move through the QA phase to draft report
- Provide objective and meaningful data to Assessors on their completed assessments

CLOSING REMARKS

As we conclude the 2025 HITRUST Trust Report, we reflect on the evolving landscape of information security and assurance. The data and insights shared in this report underscore a fundamental truth — trust is not static. It must be continuously earned, reinforced, and validated through rigorous standards, transparency, and a commitment to continual improvement.

HITRUST remains steadfast in its mission to provide organizations with the most reliable, relevant, and independently validated assurance framework. In 2024, we demonstrated the tangible impact of our approach — organizations leveraging HITRUST assessments continue to strengthen their security posture, reduce vulnerabilities, and mitigate risk at a rate unmatched by traditional compliance models. With the expansion of AI Security Certifications, enhanced Insights Reports, and our upcoming Continuous Assurance capabilities, HITRUST is setting new benchmarks for what it means to be a trusted assurance provider in a rapidly evolving threat landscape.

The coming year will bring new challenges, new threats, and new innovations — but one thing remains constant: the need for trust. As we move forward, we invite organizations, security leaders, and stakeholders across industries to demand more from their assurance programs — more accountability, more transparency, and more demonstrable security outcomes.

We look forward to continuing this journey together, building a more resilient, secure, and trusted digital ecosystem. Here's to a safe, successful, and secure 2025.