TRUST REPORT

Navigating the Landscape
of Trust in Information Assurance

HITRUST®

Table of Contents

Message From Leadership

Welcome to our first Trust Report.

When we started HITRUST seventeen years ago, our goal was to address the information compliance and security needs of the healthcare industry including those embodied in HIPAA. What we've built since then extends far beyond that initial scope. Today, HITRUST offers a comprehensive suite of security, compliance, and risk management solutions that serve a wide array of industries, not just healthcare. Our offerings are designed to be accessible, scalable, and suitable for organizations of any size, from small startups to large enterprises, enabling trust in digital systems both internally and between parties.

The breadth of our certifications, from essential to rigorous levels, reflects our understanding that there is no one-size-fits-all in information security. Our approach allows for a pragmatic journey through our traversable portfolio, ensuring that organizations can find a pathway that fits their unique needs and grows with them.

These past few years, we've observed a significant increase in the demand for our certifications. This trend suggests a shift in the industry's mindset: merely checking compliance boxes is no longer sufficient. Organizations are increasingly seeking ways to genuinely lower their risks while providing reliable evidence of their security posture. It's clear that there's a growing recognition of the value in a complete and comprehensive solution that involves the entire ecosystem—something only HITRUST provides.

Our commitment is to establish trust in the security, privacy, and compliance of computing infrastructures. To do this we build upon two dimensions, relevance and reliability. Relevant meaning, are the requirements we set forth relevant to the current threat landscape and the reality of the organization and its relationships? And reliability, based on the six principles of Transparency, Scalability, Consistency, Accuracy, Integrity, and Efficiency. We believe these are essential for an assurance program to be relied upon. We believe that any assurance solution that does not address these sufficiently should be questioned. These aren't just ideals. They are the necessary foundation for any trusted assurance system in today's world of escalating cyber threats and increasing personal liability for security breaches.

As we look to the future, including expanding our assurances to emerging technologies such as AI, our focus remains on providing the necessary tools and certifications that support your cyber risk management and compliance objectives.

Finally, we also feel that those relying on our assurances should have visibility into the checks and balances in place and the effectiveness of our program, which this report that will be issued on an annual cadence aims to address.

Thank you to our customers, partners, employees, and other stakeholders who have helped make this company what it is. I am more optimistic than ever in HITRUST's future and the importance of the work we are doing together.

Sincerely,

Daniel Nutkis
Founder and Chief Executive Officer
HITRUST

Executive Summary:

Navigating the Landscape of Trust in Information Assurance

In today's rapidly evolving digital landscape, where threats loom large and compliance complexities grow, the question of trust in assurance mechanisms becomes paramount. How can organizations be certain that the assurance reports they depend on are not merely symbolic gestures but vital instruments of trust and reliability? Amidst the myriad of compliance frameworks and assurance reports, distinguishing between superficial validation and genuine security assurance is a challenge that demands urgent attention.

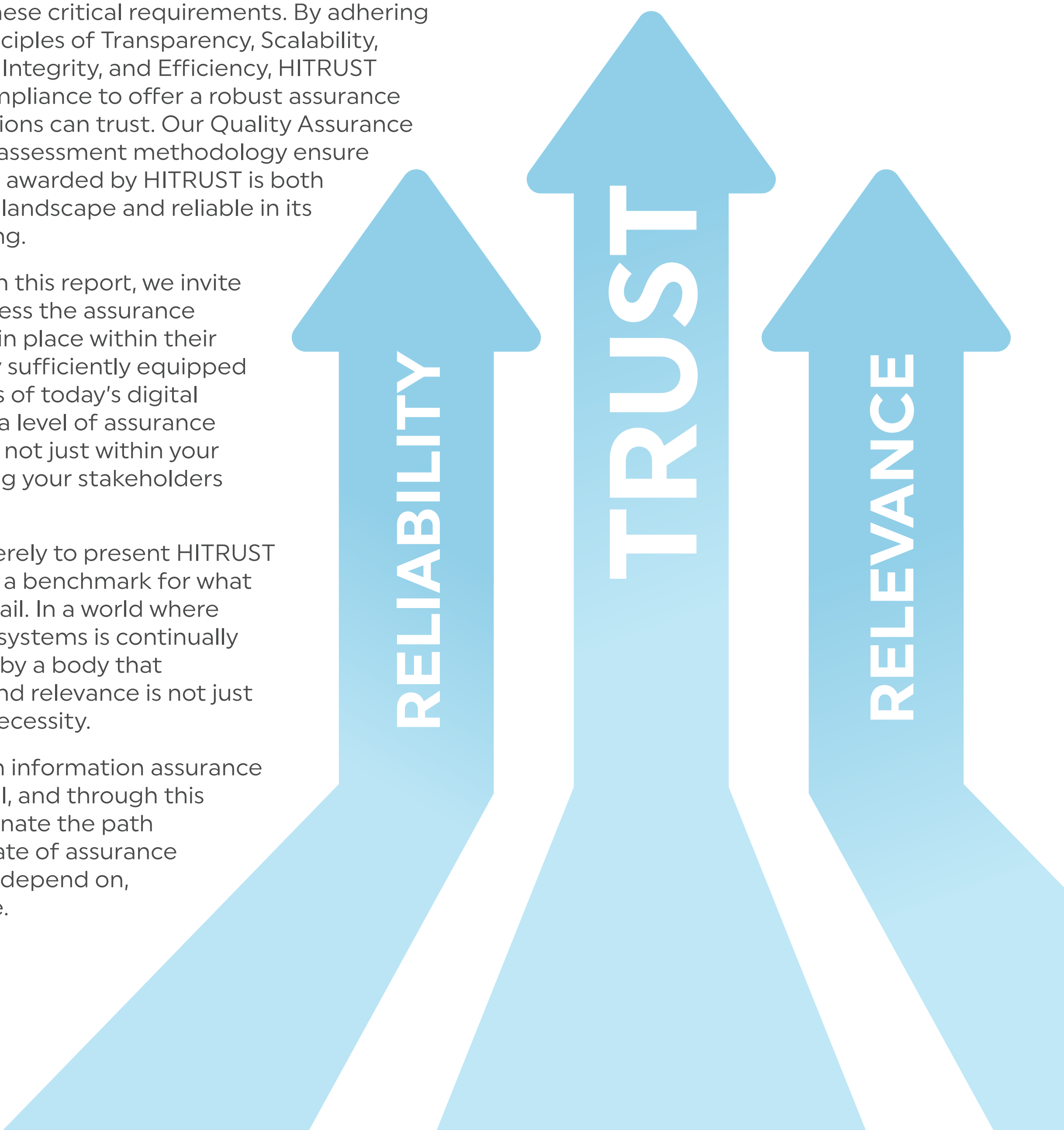
The HITRUST 2024 Trust Report seeks to address this crucial concern by presenting a comprehensive evaluation of assurance mechanisms within the context of a constantly shifting threat landscape and regulatory environment. We understand that for trust to be established, it needs to rest on two fundamental pillars: relevance and reliability. An assurance mechanism must not only resonate with the current threat environment and regulatory requirements but also demonstrate an unwavering commitment to precision, consistency, and integrity.

This report delves into how HITRUST, through 17 years of dedicated effort, has developed a framework and assurance program that stand at the confluence of these critical requirements. By adhering to the six essential principles of Transparency, Scalability, Consistency, Accuracy, Integrity, and Efficiency, HITRUST goes beyond mere compliance to offer a robust assurance solution that organizations can trust. Our Quality Assurance program and rigorous assessment methodology ensure that every certification awarded by HITRUST is both relevant to today's risk landscape and reliable in its evaluation and reporting.

As we navigate through this report, we invite readers to critically assess the assurance mechanisms currently in place within their organizations. Are they sufficiently equipped to address the nuances of today's digital threats? Do they offer a level of assurance that instills confidence not just within your organization but among your stakeholders and customers?

Our objective is not merely to present HITRUST as a solution but to set a benchmark for what digital trust should entail. In a world where the integrity of digital systems is continually tested, being certified by a body that epitomizes reliability and relevance is not just an advantage—it is a necessity.

We believe that trust in information assurance systems is foundational, and through this report, we aim to illuminate the path towards achieving a state of assurance that organizations can depend on, today and in the future.

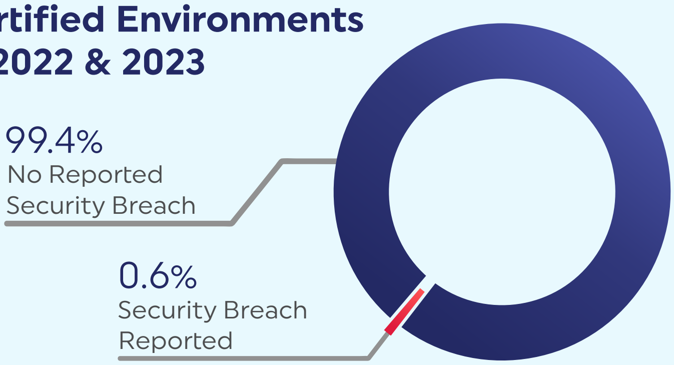


Report Highlights

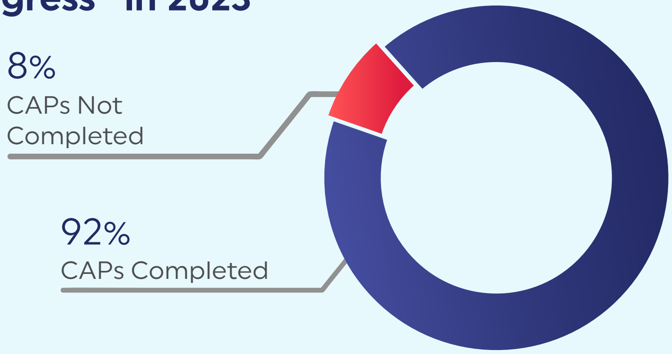
97%

of all threat indicators in MITRE ATT&CK are covered in CSF version 11.2

Breach Rate of HITRUST Certified Environments in 2022 & 2023



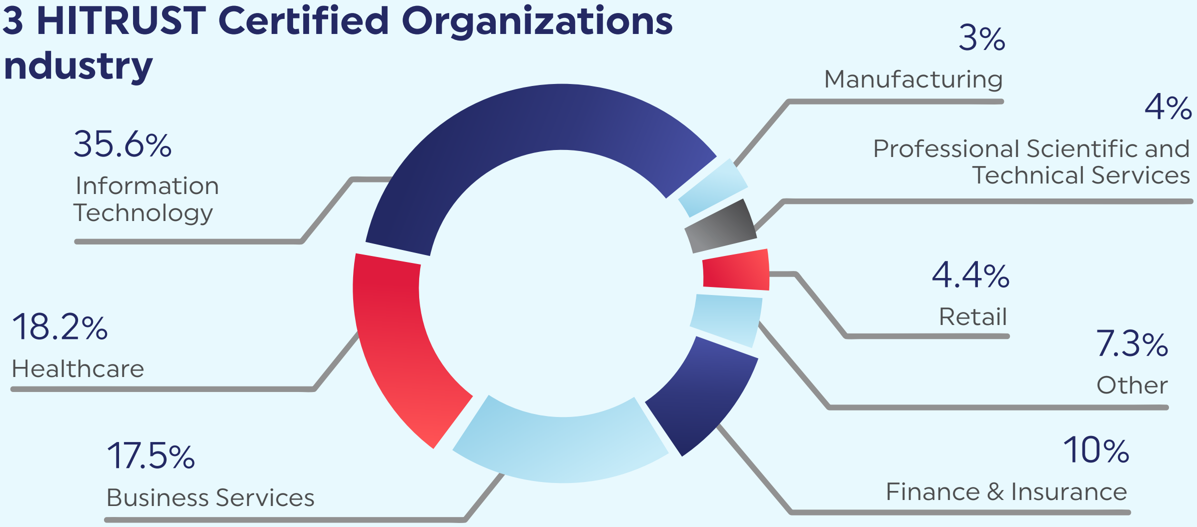
Corrective Action Plan (CAP) Progress* in 2023



*As of an organization's one-year anniversary of its r2 certification

HITRUST CSF version 11.2 incorporates **44** standards, frameworks, and regulations

2023 HITRUST Certified Organizations by Industry



100% of submitted assessments go through **HITRUST Quality Review**

HITRUST'S COMMITMENT TO A HIGH-QUALITY ASSURANCE PROCESS

HITRUST'S COMMITMENT TO A HIGH-QUALITY ASSURANCE PROCESS

Establishing trust in assurance mechanisms is challenging because many organizations do not know how to properly assess the options available. HITRUST has observed that organizations often develop a false sense of security from compliance reports and certifications that fail to offer the accurate, necessary assurances. As a result, these organizations are still vulnerable to significant information security threats.

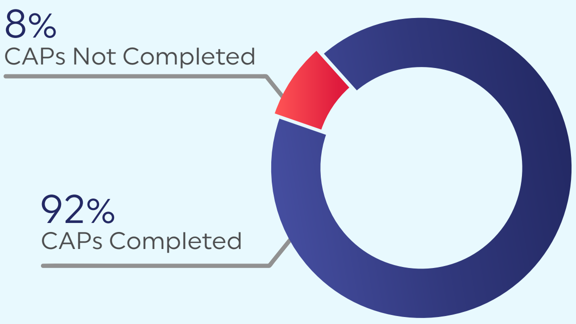
In this report, we provide expectations that you can use to evaluate whether an assurance mechanism is both **reliable** and **relevant**.

HITRUST's **reliable** assurances are built on the six essential principles of *Transparency, Scalability, Consistency, Accuracy, Integrity, and Efficiency*. HITRUST assessments encompass each of these principles and demonstrate HITRUST's commitment to a high-quality assurance process. We evolved our program to provide appropriate and transparent levels of assurance that organizations can trust. This includes incorporating a HITRUST Quality Assurance program to govern the assessment submission and report issuance processes. All assessments submitted to HITRUST must undergo a comprehensive quality review prior to achieving certification.

Relevant assurances must allow an organization to demonstrate their cyber resilience, which includes the ability to detect, protect, respond and recover from cybersecurity incidents, to a user of the report. HITRUST assessments are based upon the HITRUST CSF, which is cyber threat adaptive to ensure organizations have controls in place that address current threats, such as ransomware.

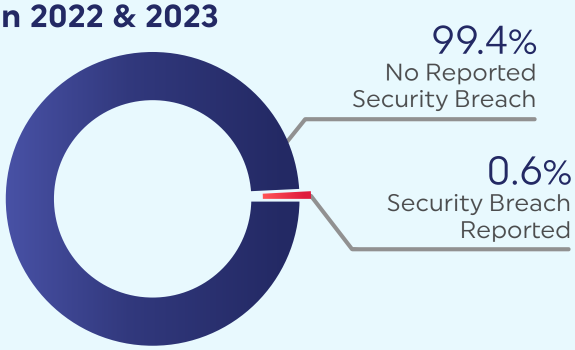
Being cyber threat adaptive means the HITRUST CSF consumes threat intelligence data from a leading threat intelligence provider, maps threats to the MITRE ATT&CK framework, and utilizes that data to identify controls within the CSF framework that are needed in an assessment. As cyber threats evolve over time, so does the HITRUST CSF, which is reviewed and enhanced to ensure new and emerging threats are mitigated.

Corrective Action Plan (CAP) Progress* in 2023



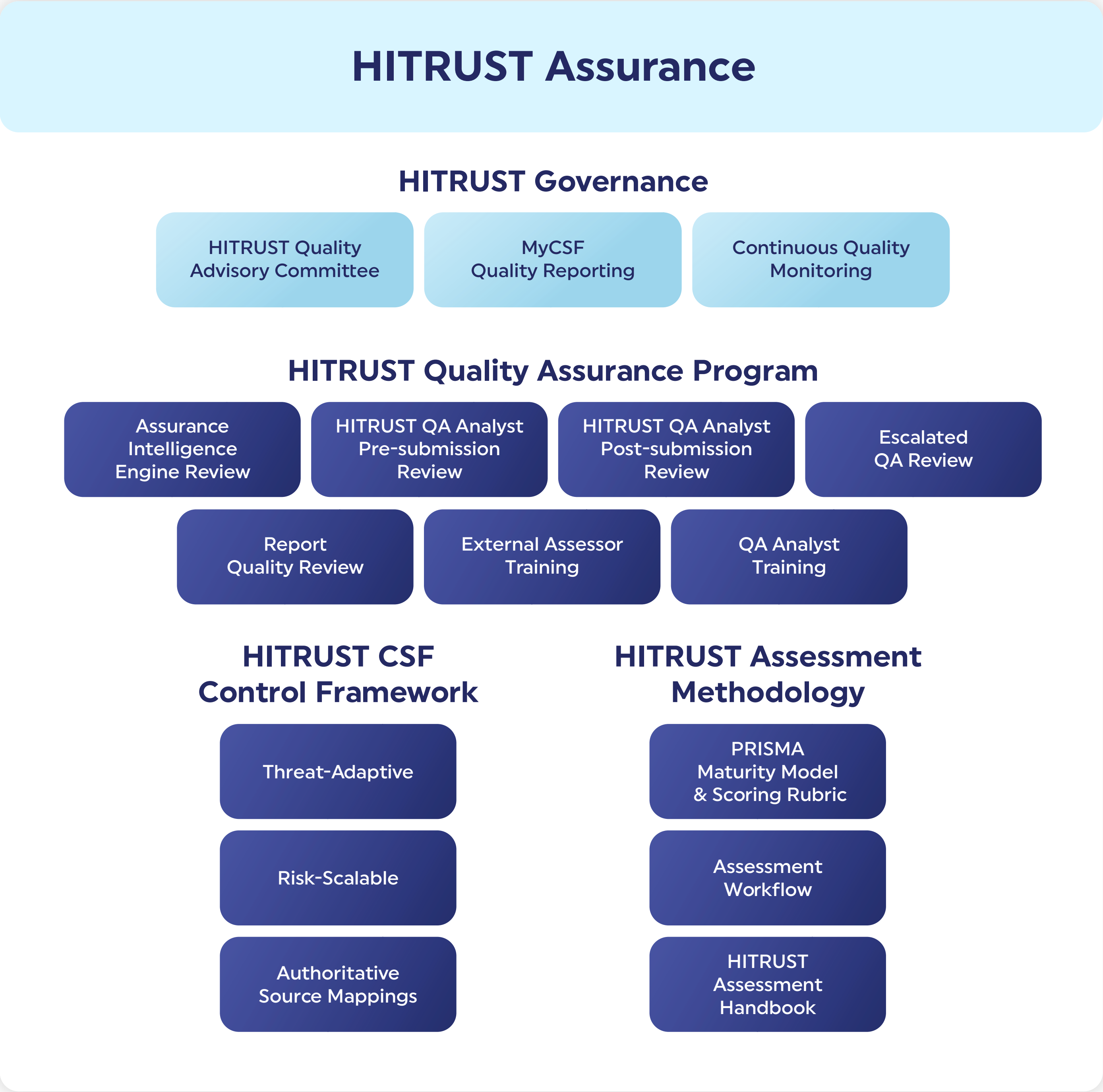
*As of an organization's one-year anniversary of its r2 certification

Breach Rate of HITRUST Certified Environments in 2022 & 2023



Through relevant and reliable assurances, HITRUST has the ability to provide assurance to the organization that it is adequately protecting and improving its information security posture over time. HITRUST believes organizations that achieve a HITRUST certification reduce their risk of a data security breach, as **less than 1% of organizations with a HITRUST certification have reported security breaches to HITRUST over 2022 and 2023**. In addition, HITRUST expects organizations to continuously improve their maturity level, even after achieving certification. In 2024, HITRUST identified that **HITRUST r2 certified organizations remediated 92% of controls that did not fully address the HITRUST CSF framework requirements within one year of achieving their certification**.

HITRUST's commitment to a high-quality assurance process starts at the top with a foundation of governance. This governance model drives continuous quality improvements within the HITRUST Quality Assurance Program, CSF control framework, and HITRUST assessment methodology. In this report, we'll further explore how each piece of the assurance process contributes to achievement of the six essential principles of *Transparency, Scalability, Consistency, Accuracy, Integrity, and Efficiency.*



HITRUST Assurance

HITRUST Governance

- HITRUST Quality Advisory Committee
- MyCSF Quality Reporting
- Continuous Quality Monitoring

HITRUST Quality Assurance Program

- Assurance Intelligence Engine Review
- HITRUST QA Analyst Pre-submission Review
- HITRUST QA Analyst Post-submission Review
- Escalated QA Review
- Report Quality Review
- External Assessor Training
- QA Analyst Training

HITRUST CSF Control Framework

- Threat-Adaptive
- Risk-Scalable
- Authoritative Source Mappings

HITRUST Assessment Methodology

- PRISMA Maturity Model & Scoring Rubric
- Assessment Workflow
- HITRUST Assessment Handbook

In addition to highlighting HITRUST's performance against each of the six essential principles, we will provide the expected components which drive reliable and relevant assurances. HITRUST believes that while other assurance providers offer assessments and frameworks that include elements supporting each principle, they are not able to offer the same high-quality assurance process that exists with HITRUST.

Principle	HITRUST Expected Components		HITRUST Performance
Transparency	Control Framework Source	A control framework must include visibility into its requirements, including the basis for the framework.	✓
	Published Assessment Methodology	A published process must exist for the assessment approach, requirements, and scoring methodology.	✓
Scalability	Tailorable Control Framework	The control framework must be customizable based on organization's needs.	✓
	Relevant Control Framework	The framework must provide controls that address the current threat landscape and adapt to the scope of the assessment.	✓
Consistency	Formal Assessor Program	There must be a mechanism to ensure a consistent approach for the firms and individuals evaluating the results.	✓
	Centralized Quality Assurance	The assurance provider must ensure consistency in its Quality Assurance process to minimize variances and inconsistencies in the report and results.	✓
Accuracy	Control Maturity Model	The assessment must be able to report the state of the organization's information protection program clearly and accurately.	✓
	Assessment Scoring Methodology	There must be a mechanism to facilitate the accurate evaluation and scoring of the organization's implemented controls.	✓
Integrity	Quality Assurance Program	A process must be in place to ensure the assessment was conducted faithfully and results reported truthfully.	✓
Efficiency	Harmonized Control Framework	The control framework must be harmonized to avoid unnecessary or redundant requirements.	✓
	Streamlined Assessment & Reporting Process	The assurance provider must be able to support an efficient assessment process and timely report issuance.	✓
	Multi-use Reporting	The reports must satisfy multiple stakeholders for multiple purposes.	✓

> **"Organizations must be able to receive relevant information they can rely on. We have identified the mechanisms needed in an assurance process to deliver that relevance and reliability. Our commitment to this assurance process is what uniquely defines the value of a HITRUST certification."**
>
> *– Vincent Bennekers, HITRUST Vice President of Quality*

Transparency

Transparency requires an assurance provider to set clear expectations of the controls necessary to achieve certification along with the certification's corresponding evaluation and scoring model. This is needed for both the organization and its report recipients to clearly understand how controls were selected, evaluated, and scored.

Control Framework Source

In the case of HITRUST validated assessment reports, the HITRUST CSF control framework is used to determine if an organization can achieve certification. This 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 to obtain certification.

HITRUST CSF version 11.2 is publicly available and incorporates 44 relevant standards, best practice frameworks, and regulations. 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.

HITRUST Authoritative Sources (as of CSF v11.2)

16 CFR Part 681 – FTC "Red Flag" Identity Theft Rules [16 CFR 681]	Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements [OCR Guidance for Unsecured PHI]	ISO/IEC 27002:2022: Information Security, Cybersecurity and Privacy Protection – Information Security Controls ISO/IEC 27002:2022]
201 CMR 17.00 – State of Massachusetts Data Protection Act: Standards for the Protection of Personal Information of Residents of the Commonwealth [201 CMR 17.00]	Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook – Information Security, Sept ember 2016 [FFIEC IS]	ISO/IEC 27799:2016: Health Informatics – Information Security Management in Health using ISO/IEC 27002 [ISO/IEC 27799:2016]
American Institute of Certified Public Accountants (AICPA) Trust Services Principles and Criteria: Security, Confidentiality and Availability, 2017 [AICPA TSP 100]	Federal Risk and Authorization Management Program (FedRAMP) [FedRAMP]	ISO/IEC 29100:2011: Information Technology – Security Techniques – Privacy Framework [ISO/IEC 29100:2011]
Asia-Pacific Economic Cooperation (APEC) Cross Border Rules for the APEC Privacy Framework, 2005 [APEC]	Health Industry Cybersecurity Practices (HICP)	ISO 31000: Risk management – Guidelines [ISO 31000:2018]
California Consumer Privacy Act (CCPA) [CCPA 1798]	Health Information Trust Alliance (HITRUST) De-Identification (De-ID) Framework: De-identification Controls Assessment (DCA) [HITRUST De-ID Framework v1]	Joint Commission Standards, The Joint Commission (formerly the Joint Commission on the Accreditation of Healthcare Organizations) [TJC]

Center for Internet Security (CIS) Critical Security Controls (CSC) v7.1: Critical Security Controls for Effective Cyber Defense [CIS Controls v7.1]	HIPAA – Federal Register 45 CFR Part 164, Subpart C: HIPAA Administrative Simplification: Security Standards for the Protection of Electronic Protected Health Information (Security Rule) [45 CFR HIPAA.SR]	Minimum Acceptable Risk Standards for Exchanges (MARS-E) v2.2: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges [MARS-E v2.2]
CMS Information Security ARS 2013 v3.1: CMS Minimum Security Requirements for High Impact Data [CMS ARS v3.1]	HIPAA – Federal Register 45 CFR Part 164, Subpart D: HIPAA Administrative Simplification: Notification in the Case of Breach of Unsecured Protected Health Information (Breach Notification Rule) [45 CFR HIPAA.BN]	New York State Department of Financial Services – Title 23 NYCRR Part 500 [23 NYCRR 500]
COBIT 5: Deliver and Support Section 5 – Ensure Systems Security [COBIT 5]	HIPAA – Federal Register 45 CFR Part 164, Subpart E: HIPAA Administrative Simplification: Privacy of Individually Identifiable Health Information (Privacy Rule) [45 CFR HIPAA.PR]	NIST Artificial Intelligence Risk Management Framework [NIST AI RMF 1.0]
Electronic Health Network Accreditation Commission (EHNAC) [EHNAC]	IRS Publication 1075 v2021: Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for protecting Federal Tax Returns and Return Information [IRS Pub 1075 (2021)]	NIST Framework for Improving Critical Infrastructure Cybersecurity v1.1 [NIST Cybersecurity Framework v1.1]
Federal Register 21 CFR Part 11: Electronic Records; Electronic Signatures, 2003 [21 CFR 11]	ISO/IEC 23894: Information technology – Artificial intelligence – Guidance on risk management [ISO/IEC 23894:2023]	NIST Special Publication 800-53 Revision 4 (Final), including Appendix J – Privacy Control Catalog: Security Controls for Federal Information Systems and Organizations [NIST SP 800-53 R4]
General Data Protection Regulation (GDPR) European Union [EU GDPR]	ISO/IEC 27001:2022: Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements [ISO/IEC 27001:2022]]	NIST Special Publication 800-53 Revision 5 Security and Privacy Controls for Information Systems and Organizations [NIST SP 800-53 R5]
NIST Special Publication 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations [NIST SP 800-171 R2]	Organisation for Economic Co-Operation and Development (OECD) Privacy Framework, 2013 [OECD Privacy Framework]	Ontario, Canada Personal Health Information Protection Act, 2004 Chapter 3 [PHIPA]
NRS: Chapter 603A – State of Nevada: Security and Privacy of Personal Information [NRS 603A]	Payment Card Industry (PCI) Data Security Standard Version 3.2.1: Information Management (IM) Standards, Elements of Performance, and Scoring [PCI DSS v3.2.1]	South Carolina Insurance Data Security Act (SCIDSA) – Title 38, Chapter 99 [SCIDSA 4655]
NY DOH Office of Health Insurance Programs SSP v5.0 [NY OHIP Moderate-Plus Security Baseline v5.0]	Personal Data Protection Act 2012 (PDPA) [PDPA]	Title 1 Texas Administrative Code § 390.2 – State of Texas: Standards Relating to the Electronic Exchange of Health Information [1 TAC 15 390.2]
Office of Civil Rights (OCR) Audit Protocol April 2016 – HIPAA Security Rule [OCR Audit Protocol (2016)]	VA Directive 6500 VA Cybersecurity Program [VA Directive 6500]	

Published Assessment Methodology

HITRUST's robust assessment approach, control maturity and scoring methodology, and related assurance requirements are also 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. On April 4, 2023, HITRUST released an exposure draft of the HITRUST Assessment Handbook. Prior to final release of the Assessment Handbook, HITRUST received and reviewed feedback from 17 External Assessor firms and other organizations. **The HITRUST Assessment Handbook (version 1.0) was published in final on October 16, 2023 and contains 401 total criteria across 15 Chapters.** It consolidates and replaces six other guidance documents HITRUST previously released.

HITRUST provides a support desk for organizations to reach out to when they have questions related to the CSF control framework, assessment approach or related assurance guidance. **In 2023, HITRUST Assurance and Quality teams resolved over 400 support tickets and provided recurring guidance to over 15 External Assessor firms.**

Assurance Provider Considerations

Do other Assurance Providers and Frameworks have the necessary components of Transparency?

Control Framework Source

A control framework must include visibility into its requirements, including the basis for the framework.

✓ HITRUST provides a published framework with the ability for an organization to cross-reference any requirement with its corresponding authoritative source.

Published Assessment Methodology

A published process must exist for the assessment approach, requirements, and scoring methodology.

✓ HITRUST maintains the publicly available HITRUST Assessment Handbook which describes the process, requirements, and scoring methodology for all HITRUST assessments.

Scalability

Scalability refers to the ability for an assurance provider to tailor its assessment approach based on organizational needs and risks. The assurance provider should also maintain a process that ensures the control framework remains relevant to the current threat landscape.

Tailorable Control Framework

HITRUST provides three assessment types for organizations:

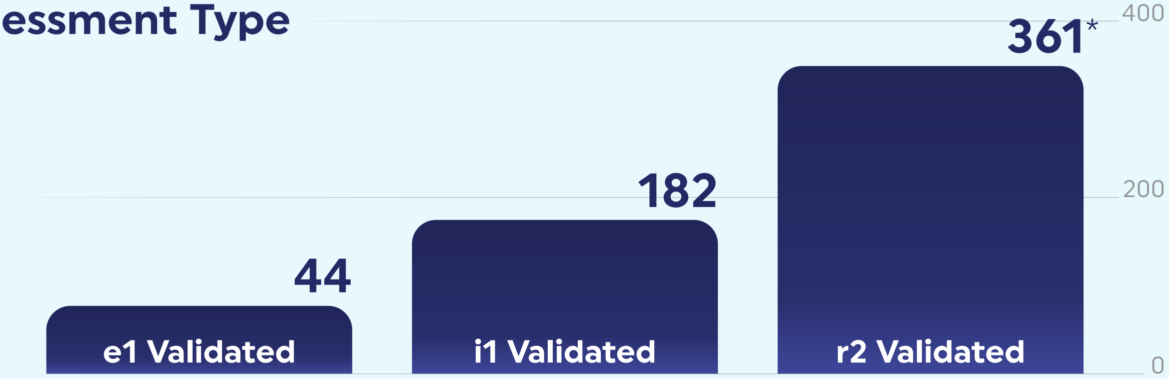
- HITRUST Essentials, 1-year (e1) Assessment: Foundational Cybersecurity
- HITRUST Implemented, 1-year (i1) Assessment: Leading Practices
- HITRUST Risk-based, 2-year (r2) Assessment: Expanded Practices

The e1 provides entry-level assurance focused on the most critical cybersecurity controls to demonstrate that essential cybersecurity hygiene is in place. **It focuses on a curated set of 44 core requirement statements, which encompass those fundamental cybersecurity practices.** These practices have been shown to represent the core controls that any organization must apply to provide a basic level of trust.

The i1 builds on those 44 requirements in the e1 by adding 138 requirement statements, which address a broader range of cyber threats. The i1 provides a moderate level of assurance through the inclusion of controls that are generally recognized as leading cybersecurity practices.

The r2 is a risk-based and tailorable assessment that provides the highest level of assurance for situations with greater risk exposure due to data volumes, regulatory compliance, or other risk factors. The r2 includes all 182 core requirements from the i1 as a baseline along with additional requirement statements based on the risk analysis HITRUST performs when an organization prepares for an r2 assessment. **In 2023, HITRUST noted that an r2 validated assessment averaged approximately 361 requirements.**

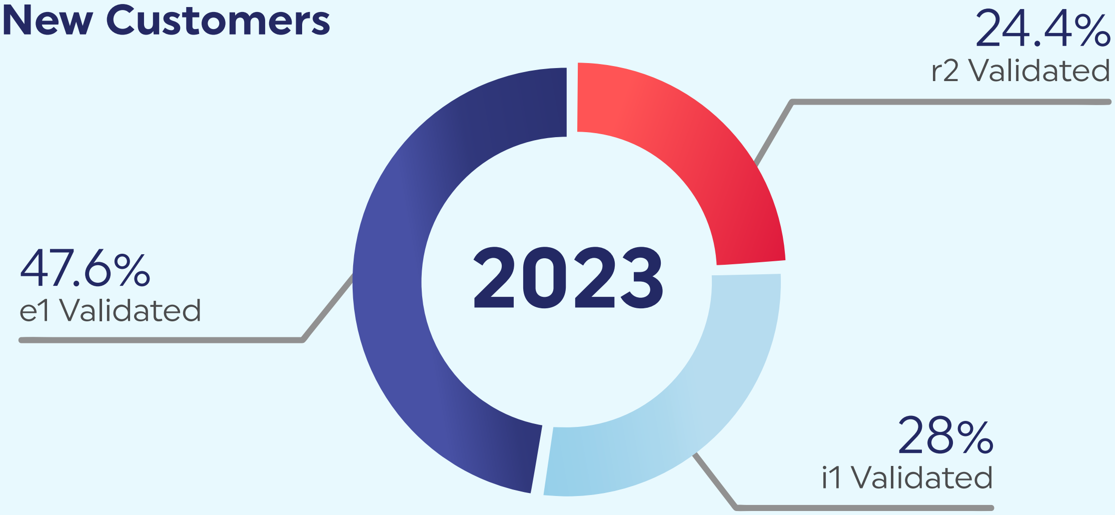
Number of Requirement Statements by Assessment Type



*Average for all r2 Validated Assessment submitted in 2023

In response to changes in market dynamics and expanded organization needs to apply HITRUST, HITRUST expanded its portfolio to meet various risk profiles. HITRUST introduced a nested portfolio across the e1, i1, and r2 on January 18, 2023 with version 11.0 of the HITRUST CSF control framework. In 2023, most new customers chose to start their HITRUST journey with the HITRUST Essentials (e1) assessment, demonstrating the market need for this type of scalability.

Assessment Types Chosen by 2023 New Customers



This market need for scalability was also represented through the increase in i1 and e1 submissions across 2023. **HITRUST noted a 187% increase in i1 validated assessment submissions from 2022 to 2023.** For the e1, HITRUST continued to see an increase in submissions quarter over quarter in 2023, including a 113% increase from Q2 to Q3 and a 58.8% increase from Q3 to Q4 2023.

Relevant Control Framework

The HITRUST CSF control framework is threat adaptive, allowing changes to the framework as the threat landscape evolves. HITRUST analyzes cyber threat data on a regular basis, comparing it to the HITRUST baseline requirements to ensure the framework includes controls to address all relevant practices and evolving cyber threats. **The i1 and r2 baseline requirements for CSF version 11.2 cover 97% of all threat indicators present in the most recent threat analysis.** Those threats not addressed in the HITRUST CSF framework cannot be mitigated (as determined by the MITRE ATT&CK framework).

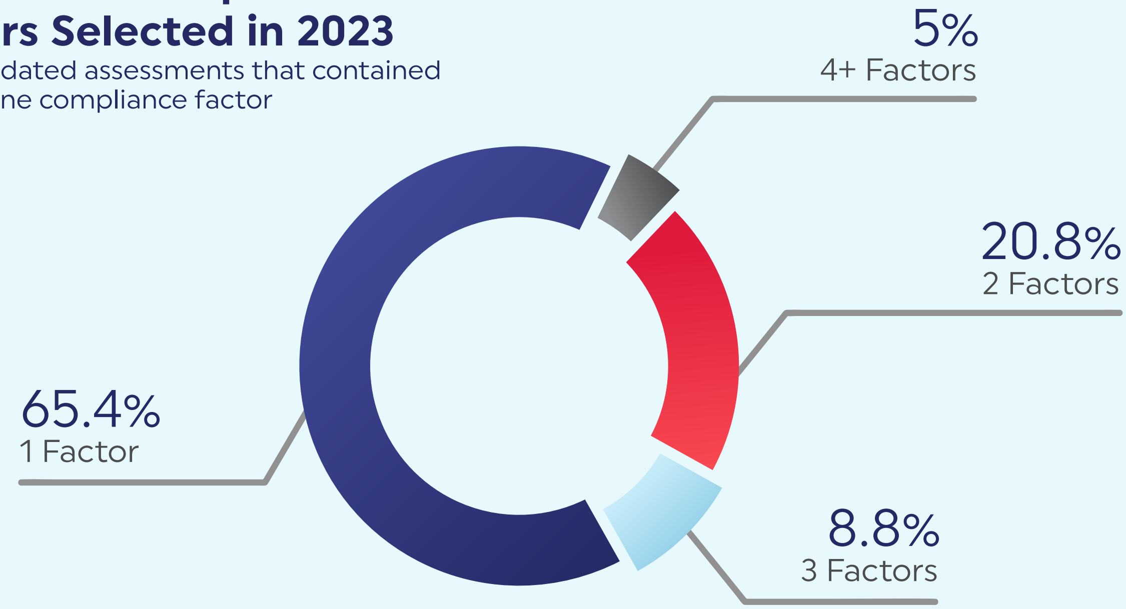
Each r2 assessment is also independently scalable through the risk analysis that HITRUST performs prior to generating the requirement statements that must be evaluated in the organization's assessment. The risk analysis uses factors to customize the assessment based on size, complexity, geography, technology, information, and regulatory requirements. The compliance factors within an assessment allow organizations to scale the assessment based on specific risks by integrating and harmonizing requirements from the relevant standards, best practice frameworks, and regulations. **Throughout 2023, over 60% of organizations selected at least one compliance factor when performing an r2 validated assessment with HIPAA being the most commonly selected factor.** For organizations that selected at least one compliance factor, over one-third selected more than one factor.

97%

of all threat indicators in MITRE ATT&CK are covered in CSF version 11.2

Number of Compliance Factors Selected in 2023

for r2 validated assessments that contained at least one compliance factor



Assurance Provider Considerations

Do other Assurance Providers and Frameworks have the necessary components of Scalability?

Tailorable Control Framework

The assurance provider must be able to customize the control framework based on organization's needs.

✓ HITRUST provides three assessment types whether the organization is ready to assess its scope against Foundational Security (e1), Leading Practices (i1), or Expanded Practices (r2).

Relevant Control Framework

The framework must provide controls that address the current threat landscape and adapt to the scope of the assessment.

✓ The threat-adaptive nature of the CSF framework allows HITRUST to maintain a continuous process for reviewing and updating its framework as threats evolve. When an organization approaches an r2 assessment, the assessment requirements are based on a risk analysis that incorporates size, complexity, geography, technology, information, and regulatory requirements.

Consistency

For an assessment to be reliable, the results must be consistent regardless of the professional or professional services firm performing the review. As a result, each assurance provider must have a process to ensure that individuals performing the work are evaluating and documenting their findings consistently. The assurance provider must also maintain an approach that minimizes variance and inconsistencies in the assessment report and results.

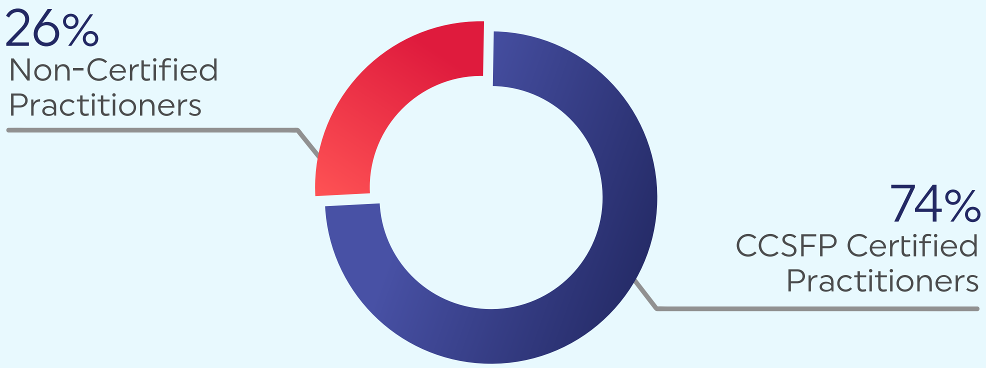
Formal Assessor Program

With the HITRUST system, 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 Assessor Program is supported by a pool of independent HITRUST Authorized External Assessor Organizations 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 of those External Assessor firms is vetted by HITRUST and required to utilize professionals who are trained and certified in the application of HITRUST's prescriptive assessment and assurance methodologies on every engagement.

HITRUST offers two certifications for individuals to demonstrate their understanding of the HITRUST CSF framework and its information protection principles: Certified CSF Practitioner (CCSFP) and Certified HITRUST Quality Professional (CHQP). The CCSFP is intended for individuals in organizations that plan to leverage the HITRUST CSF framework and process internally or External Assessors who are performing HITRUST assessments, while the CHQP provides guidance to practitioners expected to perform independent quality assurance (QA) reviews of validated assessment results. Once an individual has achieved the CCSFP designation, he/she must attend an annual refresher course to maintain the designation. **Each organization that would like to become an authorized HITRUST External Assessor must perform a minimum of 140 hours of HITRUST-specific training prior to receiving the designation.** In 2023, HITRUST provided over 37,000 hours of training to individuals through its HITRUST Academy department.

External Assessors 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 assessment quality assurance

HITRUST Assessment Hours Incurred by CCSFP Certified vs. Non-Certified Practitioners in 2023



reviewer must hold both a CCSFP and CHQP designation. That individual may not perform any other duty on the assessment to help ensure the pre-submission quality review was performed with objectivity.
In 2023, over 70% of hours on each submitted validated assessment were performed by an individual with a CCSFP designation.

Centralized Quality Assurance

HITRUST utilizes a multi-faceted approach throughout the assurance program to drive consistency in its QA process and report issuance. This includes the use of the Assurance Intelligence Engine to drive over 150 automated quality checks, along with HITRUST quality inspection through the HITRUST Assurance department.

The HITRUST Assurance department employs Analysts who perform Quality Assurance (QA) reviews on all validated assessments submitted to HITRUST. The QA Analyst is responsible for reviewing that assessments submitted to HITRUST meet HITRUST requirements prior to issuing a report and/or certification. Each HITRUST QA Analyst is expected to attend relevant training on an annual basis to maintain appropriate knowledge for their position. **In 2023, each HITRUST QA Analyst attended an average of 85 hours of training including internal HITRUST training and corresponding CPE (Continuing Professional Education) credits**.

During the QA review, the QA Analyst will open tasks when they have questions or feedback for the organization or External Assessor. **To ensure consistency in feedback across HITRUST QA Analysts, the HITRUST Quality department reviews all HITRUST QA Analysts on a monthly basis.** During the review, the HITRUST Quality team ensures 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.

Assurance Provider Considerations

Do other Assurance Providers and Frameworks have the necessary components of Consistency?

Formal Assessor Program

There must be a mechanism to ensure a consistent approach for the firms and individuals evaluating the results.

✓ HITRUST maintains a formal External Assessor program which vets all firms prior to becoming an External Assessor and requires HITRUST-specific training for each individual on an annual basis. Assessments submitted to HITRUST require a minimum percentage of hours on each assessment performed and reviewed by those individuals with HITRUST designations.

Centralized Quality Assurance

The assurance provider must ensure consistency in its Quality Assurance process to minimize variances and inconsistencies in the report and results.

✓ HITRUST uses a combination of automated quality checks and manual HITRUST quality inspection as part of a centralized Quality Assurance function to drive consistency in its QA process and report issuance.

Accuracy

Organizations expect that assessment results accurately reflect the state of controls implemented in an organization's environment. As a result, assurance providers must have mechanisms in place to facilitate the accurate evaluation and scoring of implemented controls.

Control Maturity Model

HITRUST provides the only assessment report that clearly articulates control maturity using an innovative PRISMA-based control maturity and scoring model, which 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 to sensitive information, making it the most accurate method of measuring the performance of an organization's controls. For e1 and i1 assessments, the control maturity is only scored based on the organization's information security controls implementation.

Assessment Scoring Methodology

To help assessors score control maturity in a consistent, accurate, and repeatable way, HITRUST developed a scoring rubric to be used in their scoring evaluations. **100% of validated assessments submitted to HITRUST in 2023 utilized the HITRUST scoring rubric to evaluate the organization's control maturity**.

The rubric provides guidance on scoring a requirement statement based on an evaluation of strength and coverage where strength and coverage are defined as:

- *Strength:* The rigor with which the Assessed Entity has implemented the requirement within its organization.
- *Coverage:* Percentage of the requirement where the Assessed Entity is compliant.

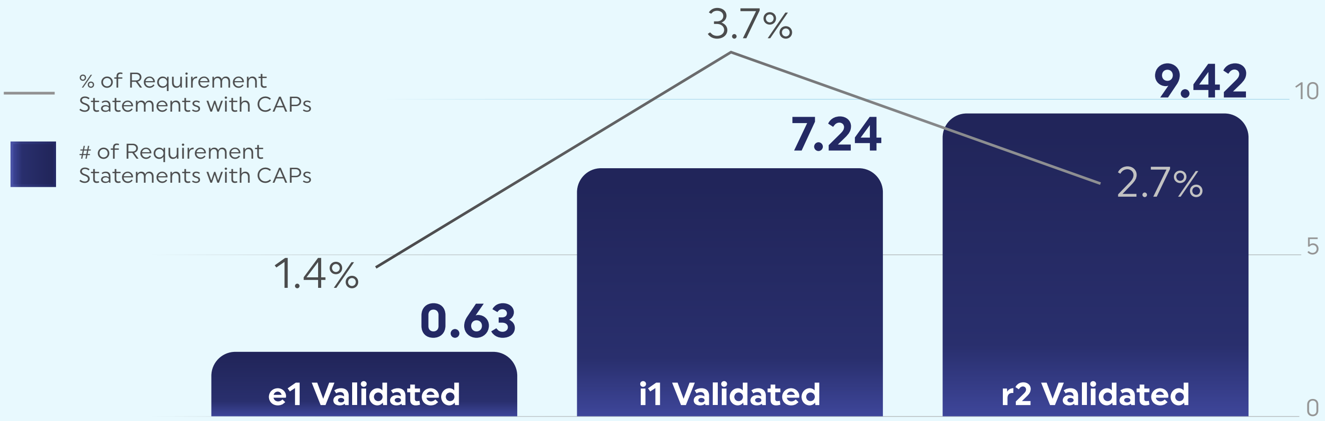
When an entity has not fully implemented a HITRUST requirement within the scope of its assessment, or when deficiencies in the operation of those controls are identified, the control maturity scores are lowered based upon the HITRUST scoring rubric. In order to achieve a HITRUST certification, each HITRUST 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.

Assessment Type	Lowest Scoring Domain
HITRUST r2 Validated Assessment	10: Password Management
HITRUST i1 Validated Assessment	19: Data Protection & Privacy
HITRUST e1 Validated Assessment	11: Access Control

If an organization's HITRUST requirement statement scores less than fully compliant and reaches a specific threshold (based on assessment type), the organization is required to define a Corrective Action Plan (CAP). The CAP must include a description of the planned corrective action that is specific, measurable, and clear enough to provide value to readers of the HITRUST report. All deficient levels and evaluative elements must be addressed by the corrective action plan. HITRUST requires CAPs so that an organization continues improving its control maturity, even if it has achieved the necessary score for certification.

HITRUST identified the average number of requirement statements along with the ratio of average number of CAPs per requirement statement for each assessment type in 2023. As the HITRUST e1 assessment is considered a cybersecurity essentials assessment, it is not surprising that it recorded the lowest average number of CAPs and CAP to requirement statement ratio. While there are more CAPs on average in an r2 validated assessment, the i1 maintained a higher CAP to requirement statement ratio across all validated assessments submitted to HITRUST in 2023. **Based on this, organizations performing an i1 average more deficiencies to remediate on a per requirement basis than those performing an e1 or r2.**

Average Number of Requirement Statements with CAPS by Assessment Type in 2023



Assurance Provider Considerations

Do other Assurance Providers and Frameworks have the necessary components of Accuracy?

Control Maturity Model

The assessment must be able to report the state of the organization's information protection program clearly and accurately.

✓ HITRUST provides the only assessment report that clearly articulates control maturity using an innovative PRISMA-based control maturity and scoring model, which provides a level of accuracy not achievable by traditional assessment approaches.

Assessment Scoring Methodology

There must be a mechanism to facilitate the accurate evaluation and scoring of the organization's implemented controls.

✓ HITRUST has developed and published a scoring rubric which assessors must use to evaluate control maturity in a consistent, accurate, and repeatable way.

Integrity

Integrity is the heart of an assessment process. Without it, an assurance provider's report cannot be trusted even if all other essential principles are in place. An assurance provider must have processes in place to ensure the assessor conducted the assessment faithfully and the results were reported truthfully.

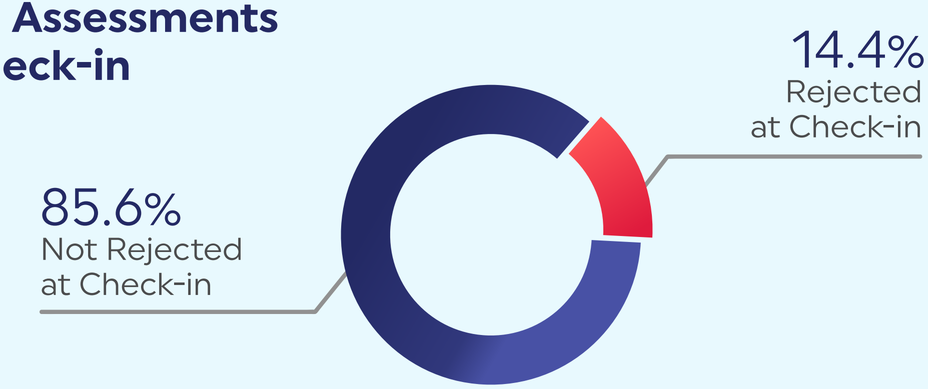
Quality Assurance Program

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 each assessment and the resulting report it produces. The key components of the quality control process include pre-submission checks, post-submission QA reviews, report quality reviews, and continuous quality monitoring.

Pre-submission checks

Utilizing the HITRUST Assurance Intelligence Engine (AIE), each submitted assessment undergoes over 150 automated quality checks to identify and address assessment errors and omissions. The Assurance Intelligence Engine proactively identifies potential issues by performing a real-time analysis against thousands of data points across the body of documentation for an assessment. Through the MyCSF platform, the Assurance Intelligence Engine provides detailed descriptions for potential quality issues, the triggering data point(s), and recommended remedial actions. Upon submission, HITRUST reviews 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.

2023 Validated Assessments Rejected at Check-in

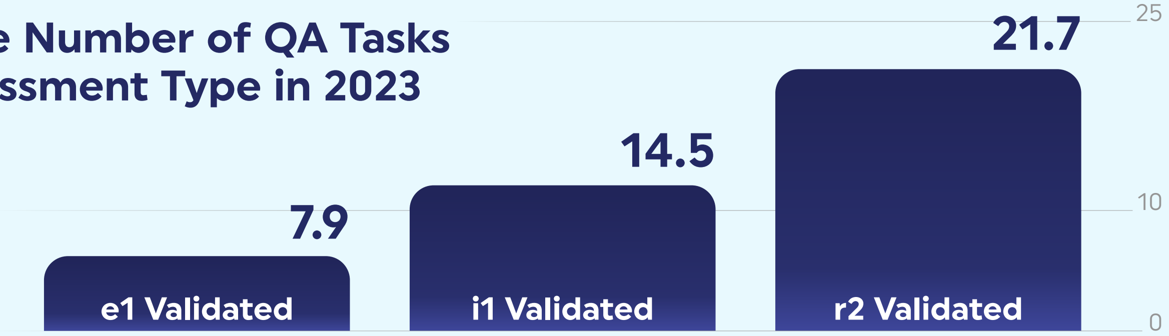


Post-submission QA reviews

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. **In 2023, HITRUST QA Analysts spent over 14,550 hours performing QA reviews on validated assessment submissions.**

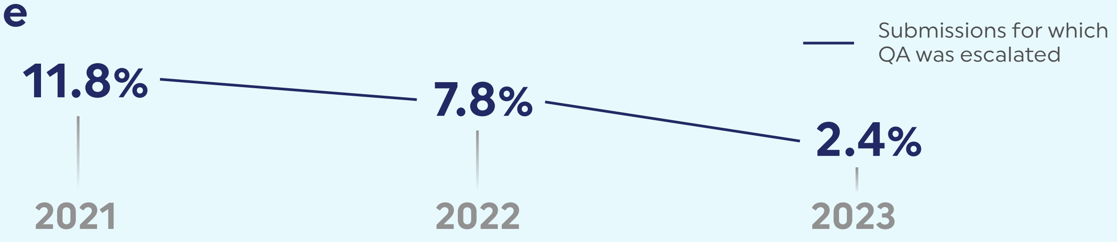
Average Number of QA Tasks by Assessment Type in 2023



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 EQA 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.

HITRUST noted a decrease in the percentage of submitted validated assessments entering EQA from 2022 (7.8%) to 2023 (2.4%). HITRUST believes the significant reduction can 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 validated assessment expectations.

Assessments Entering Escalated QA Over Time



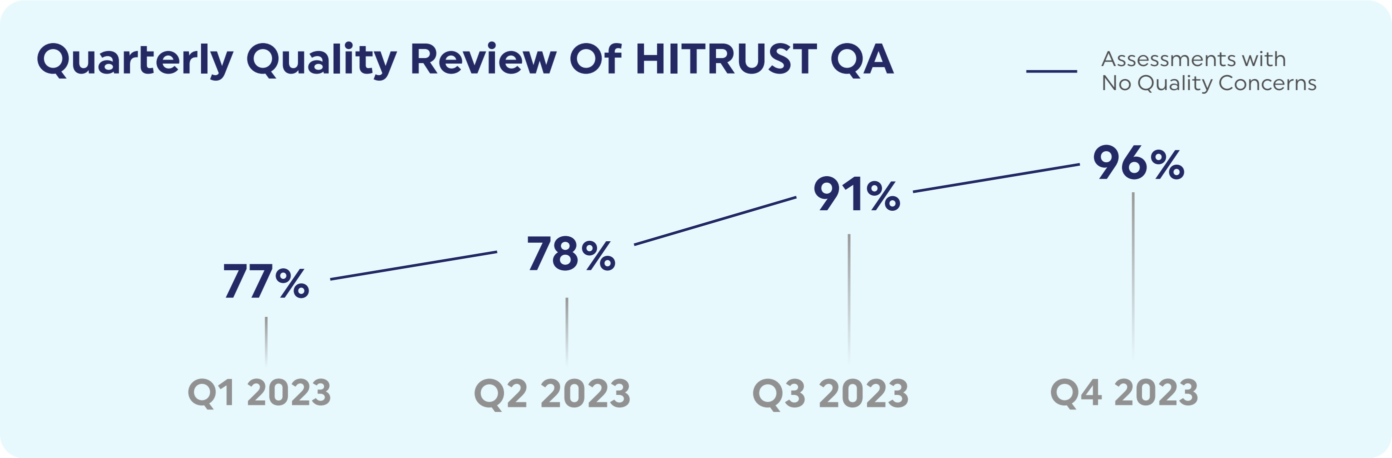
Report quality reviews

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. 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.

Continuous internal 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.

To ensure consistency in feedback across HITRUST QA Analysts, the HITRUST Quality department reviews all HITRUST QA Analysts monthly. During its review, the HITRUST Quality team ensures 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 improvement in the QA Analyst's performance throughout 2023 as it went from 77% of assessments with no quality concerns to 96% by the end of 2023.


Quarterly Quality Review Of HITRUST QA

The HITRUST Quality Assurance Advisory committee was formed to provide additional governance and 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.

Assurance Provider Considerations

Do other Assurance Providers and Frameworks have the necessary components of Integrity?

Quality Assurance Program

A process must be in place to ensure the assessment was conducted faithfully and results reported truthfully.

✓ The HITRUST Quality Assurance Program provides a granular level of oversight through a multi-layered quality control process that reviews each assessment and the resulting report it produces.

Efficiency

For a report to be efficient, assessments and their associated reports should satisfy multiple stakeholders for multiple purposes. Assurance providers should develop an assessment report that can be used by multiple relying parties. Additionally, the assessment process itself should not be burdensome with report issuance performed on a timely basis after completion.

Harmonized Control Framework

HITRUST has aligned various relevant information risk and compliance frameworks, best practices, and regulations into a single set of harmonized control requirements. In 2023, HITRUST was able to reduce the expected number of requirement statements to achieve an i1 or r2 certification through both control rationalization and control alignment with the latest cyber threat intelligence. **For an i1 assessment, CSF version 11 reduced the number of requirement statements by 17% (from 219 to 182)**. For an r2 assessment, the number of requirement statements vary based on the inherent risks present in the assessed environment (such as whether the scoped system is accessible from the internet), and the optional inclusion of compliance factors. However, HITRUST modeling of CSF version 11 projected an average requirement statement reduction of 5%.

Streamlined Assessment & Reporting Process

The MyCSF platform enables HITRUST's ability to provide an efficient approach through streamlining the assessment and reporting processes. Two key functionalities within MyCSF that support this efficiency are Inheritance and the QA Reservation System.

Inheritance

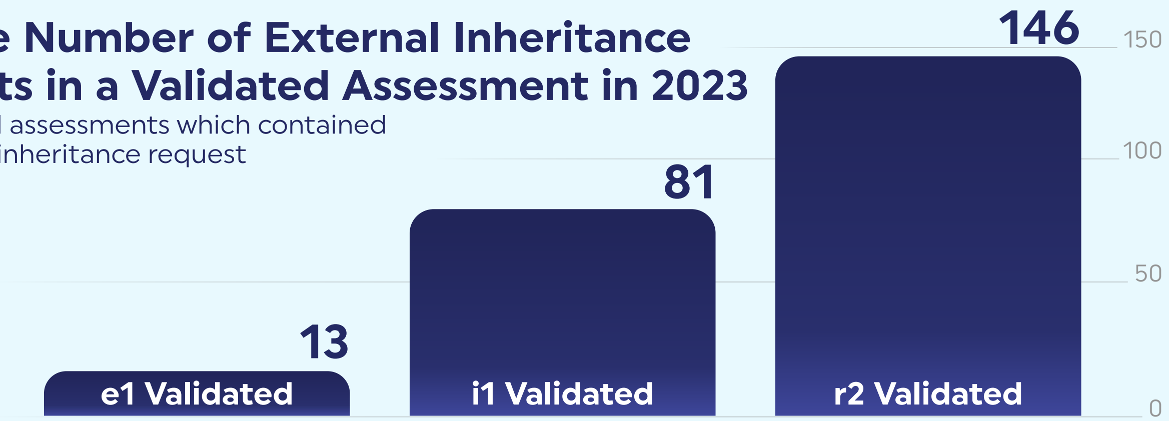
The vast majority of IT platforms built today use service providers to support various components within the platform. To adequately address the risks posed by those service providers, an organization's assessment should encompass the control performance of those providers. As a result, HITRUST developed an automated process for relying on another HITRUST validated assessment through the use of Inheritance. Inheritance allows organizations to import requirement scores from one HITRUST validated assessment into another validated assessment within the MyCSF platform. The Inheritance functionality is a simple mechanism that can be used by a service provider to share scores with users that are attempting to obtain a HITRUST certification, or it can be used by an organization to share scores across separate business units or entities. Inheritance reduces and, in some cases, eliminates the need for duplicative control assessment testing by organizations during a HITRUST assessment.

Inheritance is only possible as a result of the system of trust HITRUST has built around its assessment process. These automated reliance capabilities enable the delivery of a comprehensive assessment that addresses the risks posed by service providers.

In 2023, over two-thirds (68%) of r2 validated assessments utilized External Inheritance, while 64% of i1 validated assessments, and 58% of e1 validated assessments used External Inheritance. These organizations utilizing inheritance see both lower certification costs and faster times to achieve HITRUST certification.

Average Number of External Inheritance Requests in a Validated Assessment in 2023

for validated assessments which contained at least one inheritance request



QA Reservation System

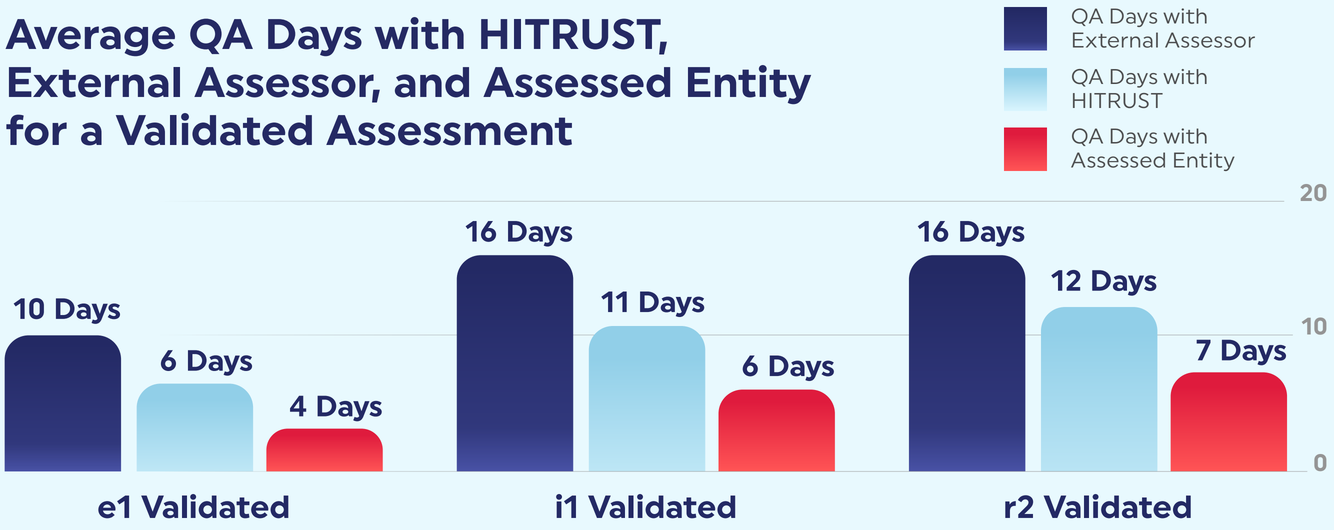
HITRUST uses an automated Reservation System within the MyCSF platform to streamline the QA process. The Reservation System requires organizations to schedule the start of their QA procedures prior to submitting a HITRUST validated assessment. The Reservation System is designed to:

- 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 on July 1, 2021, HITRUST has observed a substantial decrease in the number of days after submission when an organization will receive their HITRUST report and/or certification. 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 start to draft report for an r2 validated assessment in 2023 was 35 days.**

For i1 and e1 assessments, HITRUST has established a post-submission Service Level Agreement (SLA). The SLA commits that the HITRUST time from QA to draft report is not greater than 45 business days. If HITRUST does not meet the SLA, the organization's next i1 or e1 validated assessment report credit is complimentary. In 2023, HITRUST did not exceed this SLA threshold for any i1 or e1 assessments

Average QA Days with HITRUST, External Assessor, and Assessed Entity for a Validated Assessment



Multi-use Reporting

HITRUST's control framework incorporates 44 (CSF version 11.2) relevant standards, best practice frameworks, and regulations which allows it to deliver comprehensive assessment reports that can provide appropriate assurances for multiple requesting parties, saving organizations significant time and money—an approach HITRUST calls *Assess Once, Report Many.*

HITRUST continued to enhance its capabilities to *Assess Once, Report Many* through the introduction of Insight Reports in 2023. HITRUST Insight Reports are assurance reports that provide easy-to-understand, reliable compliance reporting over specific authoritative sources. These optional add-on reports can be produced for those organizations that have completed a HITRUST r2 validated assessment using the corresponding authoritative source. Organizations can share the reports with either internal or external stakeholders to provide its compliance posture on an authoritative source. **In November 2023, HITRUST launched the first Insight Report which includes the ability to provide insights into an organization's HIPAA compliance.** HITRUST will continue to expand its offerings in this area into 2024 to provide additional information security insights for organizations.

Assurance Provider Considerations

Do other Assurance Providers and Frameworks have the necessary components of Efficiency?

Harmonized Control Framework

The control framework must be harmonized to avoid unnecessary or redundant requirements.

✓ HITRUST has aligned various relevant information risk and compliance frameworks, best practices, and regulations into a single set of harmonized control requirements for each assessment type.

Streamlined Assessment & Reporting Process

The assurance provider must be able to support an efficient assessment process and timely report issuance.

✓ HITRUST developed the MyCSF platform to allow organizations to manage and coordinate their assessment and certification processes with assessors, service providers, relying parties and HITRUST. The Inheritance and QA Reservation System functionalities within MyCSF enable the efficient completion of an assessment and timely issuance of reports.

Multi-use Reporting

The reports must satisfy multiple stakeholders for multiple purposes.

✓ HITRUST's control framework incorporates 44 (CSF version 11.2) relevant standards, best practice frameworks, and regulations allowing it to deliver comprehensive assessment reports that can provide appropriate assurances for multiple requesting parties.

DEMONSTRATING CYBER RESILIENCE

DEMONSTRATING CYBER RESILIENCE

For an assurance mechanism to be relevant, it must allow the organization to demonstrate it has the necessary cyber resilience capabilities. These cyber resilience capabilities are necessary to allow organizations to continuously support their business operations regardless of the nature of the cyber attack.

The HITRUST CSF framework drives cyber resilience so that organizations are able to detect, protect, respond, and recover from cyber incidents. A HITRUST certification allows an organization to demonstrate it has achieved a high level of cyber resilience.

When an organization achieves HITRUST certification it remains valid from the date of certification for a specific amount of time into the future; two years for an r2 certification, and one year for an i1 or e1 certification as long as certain conditions are met during that period. These conditions include:

- No data security breach reportable to a federal or state agency by law or regulation has occurred within or affecting the assessed environment.
- Annual progress is made on areas identified in the Corrective Action Plan(s) (CAPs).
- No significant changes in the business or security policies, practices, controls, and processes have occurred that might impact its ability to meet the certification criteria.

These conditions are in place to ensure that organizations continue to meet and exceed their assessed levels of cyber resilience.

Data Security Breaches

Cyber resilience not only expects organizations are appropriately protected from cyber threats, but that when it occurs, they can detect, respond and recover from a particular security incident. When an organization achieves a HITRUST r2 certification, it has demonstrated that the organization's security program has achieved compliance with the most rigorous cybersecurity requirements that HITRUST publishes. However, no organization can fully eliminate all risks of a security breach due to the various types of threats along with weaknesses that can be exposed.

When an organization encounters a security breach, HITRUST works with the organization to understand the nature, cause, and impact of the cyber attack in relation to the scope of its assessment. HITRUST uses the reported security breach information to enhance the CSF framework as part of its cyber threat adaptability program.

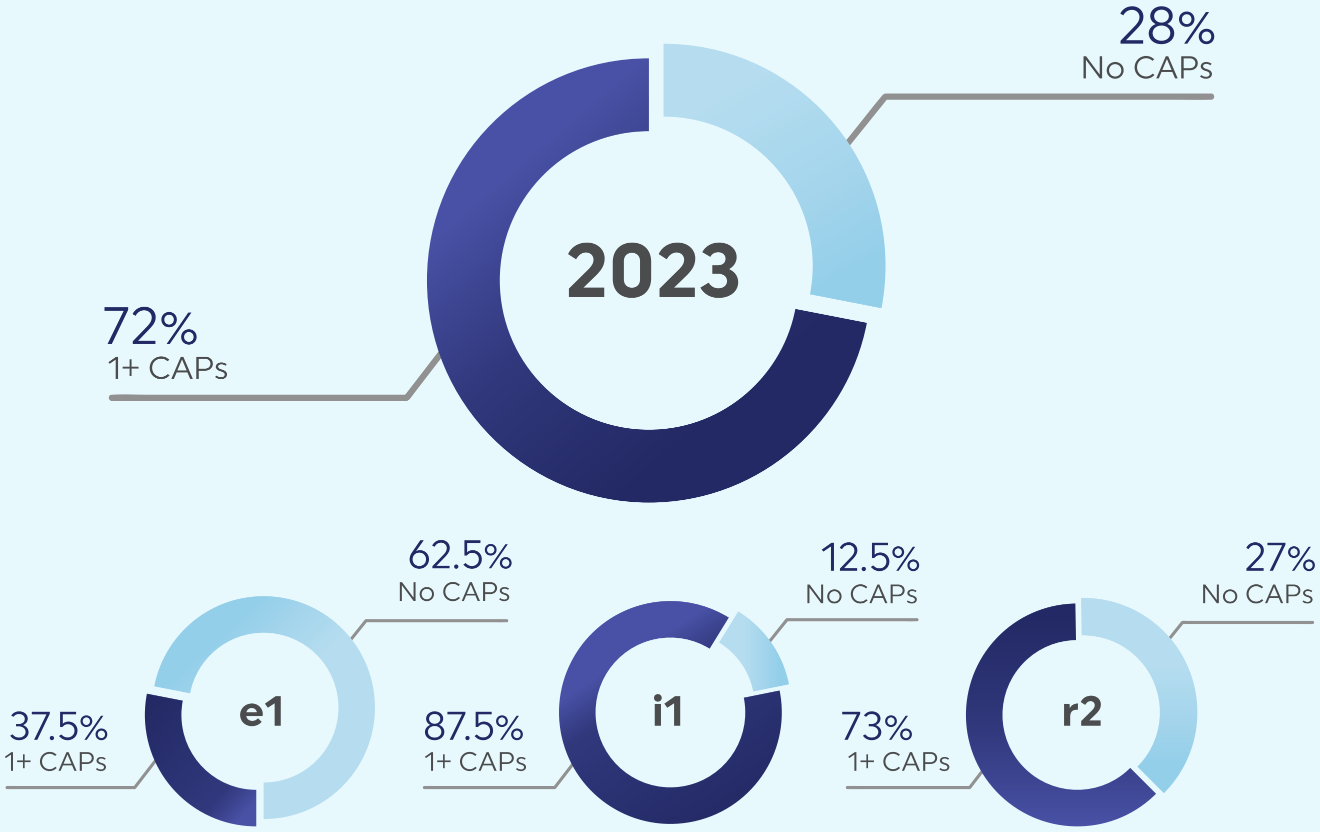
While not all risks can be fully eliminated, HITRUST believes that achieving a HITRUST certification significantly reduces the risk of a data security breach. When a HITRUST-certified organization has a security breach in the certified environment, its agreement with HITRUST requires them to notify HITRUST. **Over 2022 and 2023, only 0.64% of organizations that received HITRUST certifications reported a security breach to HITRUST in their certified environment over that same period.**

Annual Progress on Corrective Action Plans (CAPs)

HITRUST expects organizations to make annual progress on CAPs so they are not only meeting the assessed level of cyber resilience, but continuing to increase their cyber resilience capabilities. If an organization's HITRUST requirement statement scores are below a specific threshold (based on assessment type), it is required to define a CAP to improve its control maturity in that domain. This causes those organizations that have achieved a HITRUST certification to more regularly improve their security posture than those that haven't achieved a HITRUST certification.

In 2023, HITRUST identified that 28% of all validated assessments did not require a CAP to be defined. For r2 assessments with CAPs, **92% of those CAPs were closed, on average**, by the interim assessment which occurs on the one-year anniversary of a certification.

2023 Validated Assessments with Corrective Action Plans (CAPs)



Significant Changes

A HITRUST certification is only valid for the environment included in-scope of the organization's assessment and the corresponding certification letter and validated report. However, HITRUST understands that Assessed Entities may have fast-changing environments that still require maintaining a continuous HITRUST certification. As a result, HITRUST has a collaborative process that enables Assessed Entities to maintain their certification when they have identified developments that may impact their current certification. **In 2023, 2.1% of certified organizations reported a significant change to HITRUST.** HITRUST provided guidance for each of those entities on the steps and testing necessary for their HITRUST certifications to remain in compliance.

> **"Organizations have discovered that HITRUST assessments are the gold standard in information protection assurances because of the comprehensiveness of control requirements, depth of quality review, and consistency of oversight. The tools and methodologies used by organizations to complete HITRUST certification allow them to assess and report against multiple sets of requirements – assess once, report many, as we say – making our certification assurances efficient, transparent, and thorough."**
>
> – *Bimal Sheth, HITRUST Executive Vice President, Standards Development & Assurance Operations*

THE HITRUST MYCSF PLATFORM

THE HITRUST MYCSF PLATFORM

HITRUST developed the MyCSF platform to integrate all stakeholders into the system of trust that HITRUST has built. The HITRUST MyCSF platform allows an organization to manage its assessment and certification through coordination with its assessor, service providers, relying parties, 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 framework utilizing functionality that incorporates the essential principles for a reliable and accurate assessment report including:

- Assessment Workflow
- Assurance Intelligence Engine
- Inheritance
- Results Distribution System (RDS)

"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. We will continue to develop and streamline our assurance processes providing organizations with numerous quality advantages over other assurance programs and certifying bodies."

– Jeremy Huval, HITRUST Chief Innovation Officer

Assurance Provider Considerations

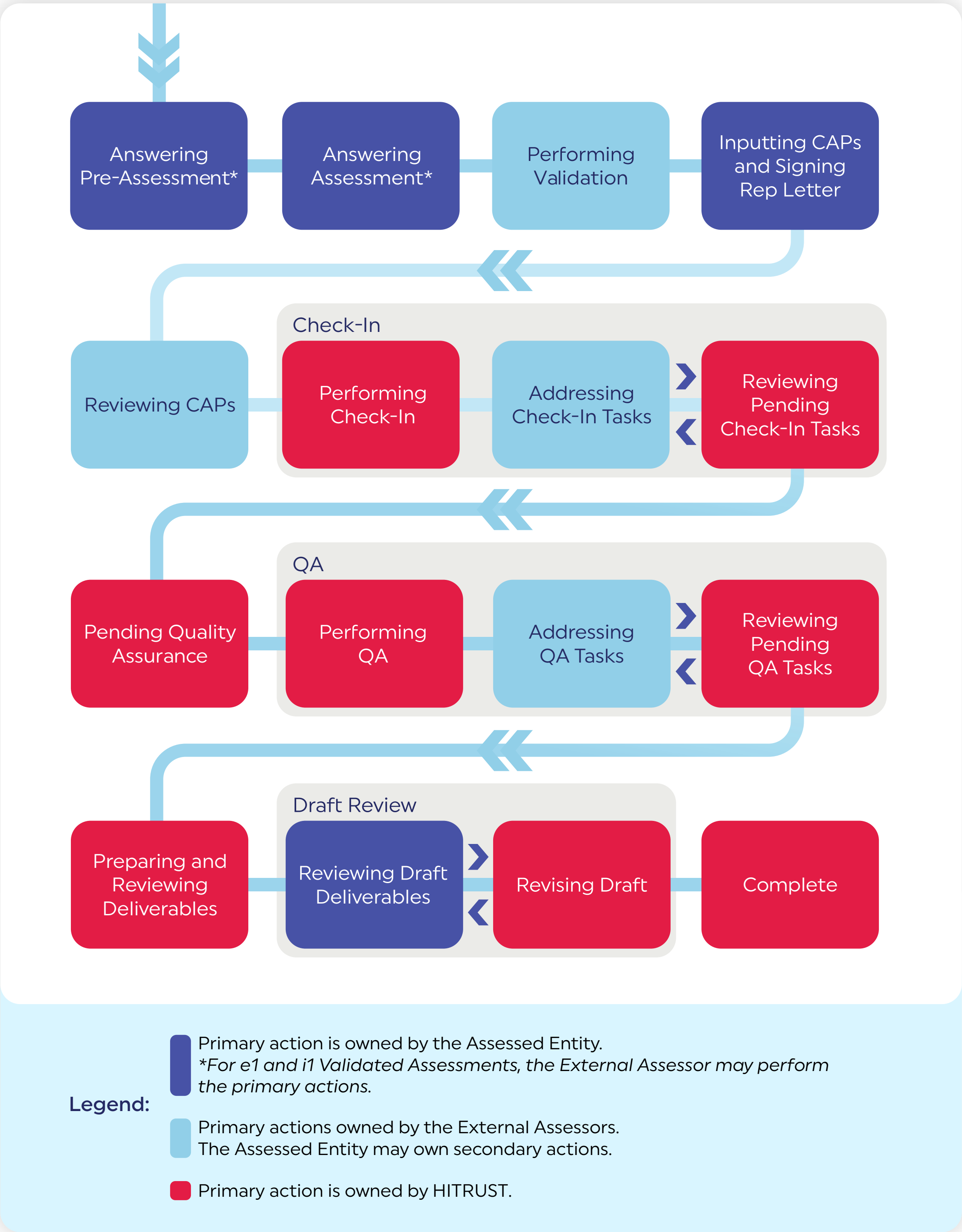
Do other Assurance Providers and Frameworks have platforms that allow organizations to manage and coordinate their assessments and certifications?

✓ The HITRUST MyCSF platform allows an organization to manage and coordinate its assessment and certification processes with assessors, service providers, relying parties, and HITRUST.

Assessment Workflow

The workflow for any HITRUST assessment consists of multiple workflow phases with each phase owned by either HITRUST, the organization being assessed, or the External Assessor. MyCSF automates the entire workflow and submission process for these assessments. When a workflow phase is complete, the entity owning the phase is able to submit the assessment into the next phase of the workflow. When entering a new phase, entities will receive notifications that the assessment has moved into the next phase in the workflow.

HITRUST Validated Assessment Workflow Phases



Answering Pre-Assessment*
Answering Assessment*
Performing Validation
Inputting CAPs and Signing Rep Letter
Check-In
Reviewing CAPs
Performing Check-In
Addressing Check-In Tasks
Reviewing Pending Check-In Tasks
QA
Pending Quality Assurance
Performing QA
Addressing QA Tasks
Reviewing Pending QA Tasks
Draft Review
Preparing and Reviewing Deliverables
Reviewing Draft Deliverables
Revising Draft
Complete
Legend:

Primary action is owned by the Assessed Entity.
For e1 and i1 Validated Assessments, the External Assessor may perform the primary actions.

Primary actions owned by the External Assessors.
The Assessed Entity may own secondary actions.

Primary action is owned by HITRUST.

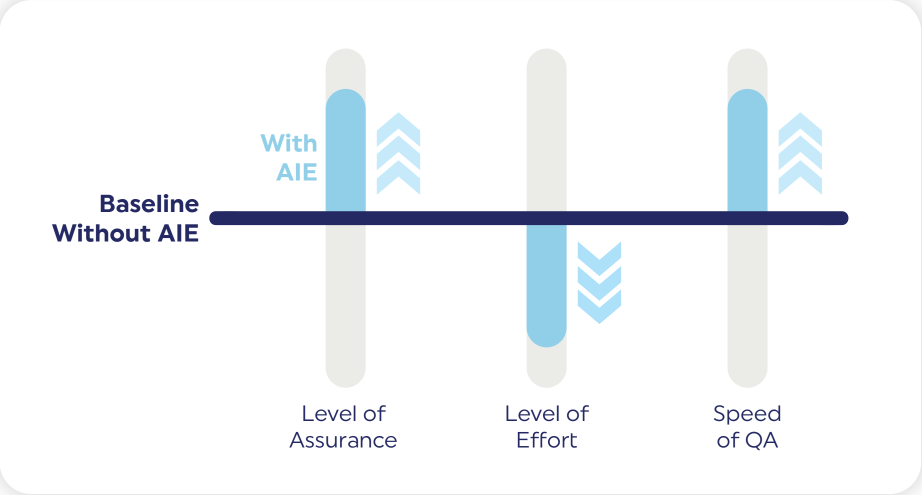
The MyCSF platform also includes a Kanban-style dashboard allowing all participants of the assessment to track and view the assessment status at any time. The Kanban view contains a column for each phase of the Validated Assessment Workflow, and each accessible Validated Assessment is displayed as a card. The view includes key details of each Validated Assessment, including:

- Colored, circle badges depicting responsible parties for action items
- Summary of open items per organization
- Time elapsed in current phase
- HITRUST-assigned point of contact

Assurance Intelligence Engine

MyCSF also includes the Assurance Intelligence Engine (AIE) to drive efficiency and elevate quality. The AIE analyzes assessment documentation for oversights, inconsistencies, and errors throughout the information security and privacy assessment process. It adds efficiency to the HITRUST assessment quality review process by adding a layer of automated checks that complement existing, manual reviews to identify potential issues in assessment submissions that might otherwise jeopardize the integrity, accuracy, or consistency of information.

Impact of the Assurance Intelligence Engine™ on the HITRUST CSF Assurance Program



Prior to an assessment moving into the next workflow phase, the AIE will notify the participant of errors (or potential errors) in the corresponding information entered into MyCSF. The AIE brings awareness for early remediation of quality issues and this awareness also helps to avoid their recurrence. It adds efficiency to the entire assurance lifecycle by reducing the likelihood of surprises during quality assurance reviews of completed assessments. The impacts are mutually beneficial for HITRUST, organizations, and External Assessors.

Inheritance

Inheritance is a unique capability available in MyCSF that delivers a high-efficiency solution to streamline the process and expense of managing information protection assurance assessments. Inheritance can be used internally to import control testing results and scores from an organization's HITRUST validated assessment, or externally from a third-party HITRUST-certified cloud or other service provider who shares responsibility for protecting an organization's data.

Key Inheritance Benefits

Reduces the need for duplicative and redundant direct controls testing that is covered and obtained under a prior valid assessment.

Identifies control mappings and leverages assessment results within one system to efficiently process inheritance information exchange.

Provides the transparency and visibility needed to fully understand and effectively inherit existing controls assessment data.

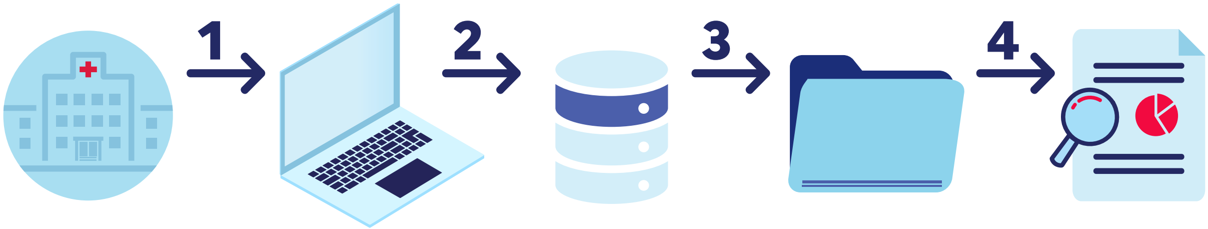
The industry's only inheritance capability for third-party assurances, especially well-suited for shared cloud-based control environments.

The MyCSF platform works in determining what controls are inheritable, validating the applicability of Inheritance requests to the scope of the assessment, orchestrating the exchange, and managing the process. This dramatically reduces the level of effort for all involved. By working with a participating service provider, customers can reduce the required testing and associated costs for inherited controls in a fully automated manner.

With external inheritance, organizations of all sizes and levels now have the ability to leverage cloud platforms to their utmost potential because HITRUST has worked with service providers to accept full or partial responsibility for delivering on many security control objectives on behalf of their customers. This gives customers and service providers a complete understanding of which parties are responsible for which controls.

Results Distribution System (RDS)

RDS makes it possible for assessed entities to share results from their HITRUST assessments securely and electronically with any relying party. Those recipients can then manage and review essential information—such as assessment date, scope, control requirements, scores, corrective action plans (CAPs), and more—using the API (Application Programming Interface) and their own TPRM (Third-party Risk Management) solution. This automation adds efficiency and saves time by eliminating the multiple back-and-forth communications that are common between parties during the annual vendor review process. Whether relying parties manage hundreds or thousands of vendors, RDS delivers game-changing innovation and efficiencies.



Results Distribution System Reliant Party Ecosystem

1. Reliant party requests Assessment Data through API from HITRUST
2. Reliant party granted access to Supplier Assessment Data
3. Reliant party enhances current data in their VRM/TPRM/GRC solution
4. Reliant party manages residual risk associated with entire supply chain through enhancement of supplier assessment data

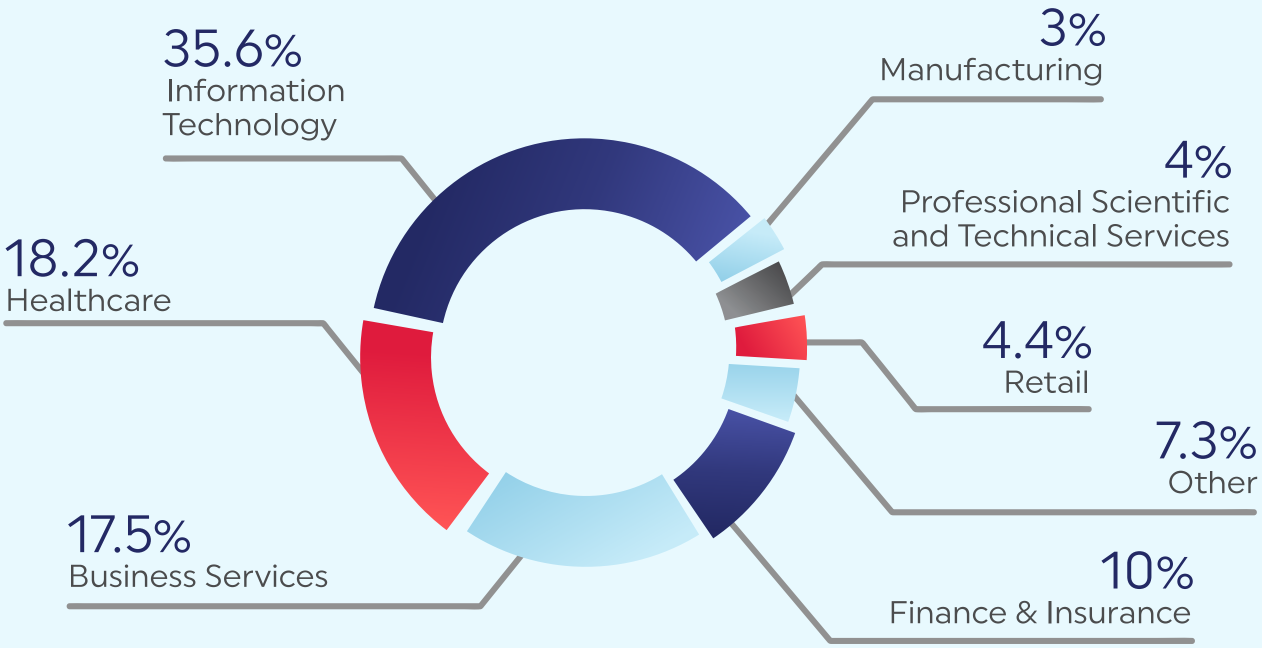
LOOKING AHEAD

LOOKING AHEAD

Since it was 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 continuously broadens the ability for organizations of all sizes and industries to utilize and benefit from a HITRUST assessment. In 2023, HITRUST noted the top five industry sectors that obtained a HITRUST certification were:

- Information Technology
- Healthcare
- Business Services
- Finance & Insurance
- Retail

2023 HITRUST Certified Organizations by Industry



HITRUST expects to continue to broaden its industry base in 2024 through additional initiatives to enhance the ability for organizations to leverage a HITRUST report.

PLUS Reporting & Insight Reports

In 2024, HITRUST will expand the scope of available validated assessments through the ability to select, or tailor, additional authoritative sources for validation on top of the HITRUST e1 Essentials and HITRUST i1 Implemented assessments. These "e1 PLUS" and "i1 PLUS" reports will expand the e1 and i1 reports with the same tailoring logic used by the HITRUST r2 Risk-based assessment—providing increased flexibility and value for organizations with multiple security and compliance requirements—all with the same transparency, scalability, consistency, accuracy, and integrity provided with all HITRUST assurance reports.

In order to support the new and increased flexibility and relevance available for all HITRUST assurance reports, HITRUST will release a series of Insight Reports throughout 2024. These reports will extend the Insight Reports concept beyond the three HIPAA Insight Reports available today to a portfolio that allows organizations that have completed e1 PLUS, i1 PLUS, or r2 validated assessments to understand and report on their coverage and conformity with the many authoritative sources available through the HITRUST framework.

The scalability and flexibility of these reports will support customers from many different industries across the globe. All PLUS Reports and Insight Reports will build on the HITRUST pillars of relevance and reliability. These new assurance mechanisms will continue to be backed by an industry leading Quality Assurance Program and the nested approach to assurance reporting that supports an organization's needs both today and throughout their security and compliance journey.

HITRUST Artificial Intelligence (AI) Assurance Program

AI, and more specifically, Generative AI, made popular by OpenAI's ChatGPT, is unleashing a technological wave of innovation with transformative economic and societal potential. Goldman Sachs Research predicts that Generative AI could raise global GDP by **7% over the next 10 years**. Organizations are eager to transform their operations and boost productivity across business functions ranging from customer relationship management (CRM) to software development in order to unlock new layers of value through a growing evolution of enterprise AI use cases. However, any new disruptive technology also inherently delivers new risks, and Generative AI is no different.

AI foundational models now available from cloud service providers and other leading organizations allow organizations to scale AI across industry use cases and specific enterprise needs. But the opaque nature of these deep neural networks introduces data privacy and security challenges that must be met with transparency and accountability. It is critical for organizations offering AI solutions to understand their responsibilities and ensure that they have reliable assurances for their service and solution providers.

As a result, HITRUST is launching the AI Assurance Program: the first and only assurance program able to demonstrate and enable sharing of security control assurances for Generative AI and other emerging AI model applications.

HITRUST began prioritizing AI Risk Management as a foundational consideration with the release of HITRUST CSF version 11.2 in October 2023. In this release, HITRUST included an "Artificial Intelligence Risk Management" compliance factor which included mappings to the following authoritative sources:

- NIST AI Risk Management Framework (RMF) v1.0,
- ISO/IEC 23894 (AI Risk Management Guidelines), and
- ISO 31000

This provides an important foundation that AI system providers and users can use to consider and identify risks and negative outcomes in their AI systems with regular updates available as new controls and standards are identified and harmonized in the framework and available through HITRUST assurance reports.

HITRUST will add an AI certification so that organizations can address AI risks through a common, reliable, and proven approach.

This will allow organizations that are implementing AI systems and the AI model and service providers to understand the risks associated and reliably demonstrate their adherence with AI risk management principles with the same transparency, consistency, accuracy, and quality available through all HITRUST reports.

AI certifications will be supported on top of the HITRUST e1, i1, and r2 reports. This allows organizations to provide assurances that they have considered risks from their adoption and use of AI while also demonstrating the maturity of the underlying system that supports the AI platform.

HITRUST Compliance Insight Reports will also be available to support organizations that wish to demonstrate the breadth, coverage, and quality of their AI Risk Management efforts to relying parties, including customers, that are seeking to understand efforts that the organization has undertaken to understand and manage AI risks and to govern their AI systems in a trustworthy, responsible, and reliable manner.

The use of existing and proven HITRUST reports and the HITRUST assurance system will demonstrate that the security of the underlying technology systems supporting the AI system has also been considered including transparency around the identification and documentation of risks, consistency in assessment results, and independent verification and quality assurance of the testing.

> **"Trustworthy AI requires understanding of how controls are implemented by all parties and shared and a practical, scalable, recognized, and proven approach for an AI system to inherit the right controls from their service providers. We are building AI Assurances on a proven system that will provide the needed scalability and inspire confidence from all relying parties, including regulators, that care about a trustworthy foundation for AI implementations."**
>
> *– Robert Booker, HITRUST Chief Strategy Officer*