THE ASSURANCE GAP

HITRUST®

Table of Contents

Executive Summary

Third-party risk management (TPRM) teams need scalable ways to evaluate vendors, while vendors need credible ways to demonstrate trust without answering a different questionnaire for every customer. The market has responded with a wide range of reports, certifications, frameworks, registries, and self-assessments. The problem is that these artifacts are often treated as interchangeable even though they were designed to serve different purposes.

Too often the assurance artifact is not a good match to cover the recipient's actual risk, creating an *assurance gap*. A report can be professionally prepared and still be insufficient when the assessed scope does not match the service being used; when important controls are optional, broadly stated, or not described; when subservice organizations are not included in scope; when the assessment does not adapt to current threats; or when the results cannot be compared across vendors without extensive interpretation.

HITRUST, SOC 2, ISO 27001, NIST Cybersecurity Framework, PCI DSS, and questionnaires each serve a distinct purpose. The right mechanism depends on the decision being made, services and data in scope, the threat exposure, the level of independence required, and how much reliance the recipient intends to place on the result.

Two of the most commonly used assurance artifacts in TPRM are SOC 2 reports and security questionnaires. Questionnaires are frequently organization-specific, with no single governing body prescribing their content, evidence requirements, or validation methods.

Evaluating Assurance Artifacts

A third-party risk management program should not begin with the question, "Which artifact does the vendor have?". Rather they should ask, "What risk decision must we make, and what evidence would justify that decision?"

The program can then evaluate the artifact through five questions:

- Does the scope cover the provided service?
- Is the assurance report responsive to the expected risks and threats?
- Who prepared and quality reviewed the work?
- What service providers are included and are they assessed?
- Can two reports be measurably compared?

These questions are a way to identify **what an assurance artifact supports, what it does not support, and what supplemental work is required.**

This lack of standardization makes questionnaires difficult, if not impossible, to benchmark consistently across organizations. It represents both a persistent operational challenge for TPRM teams and a methodological limitation for analysis. Accordingly, while questionnaires remain an important tool for collecting decision-specific information and filling gaps left by reusable assurance reports, our analysis focused on SOC 2, a widely accepted mechanism with a defined framework and a sufficiently consistent body of reports to support structured evaluation.

SOC 2: WHAT IT IS, AND WHAT IT IS NOT

SOC 2 should be understood within the context of its original design. The AICPA designed System & Organization Controls (SOC) reporting to provide customers and business partners with information useful for assessing risks associated with outsourced services. However, a SOC 2 report is not intended to serve as universal assurance around information security as it is often being used by its report recipients today. A SOC 2 report can provide detailed, decision-useful information, but only when the reader has the expertise and time to review scope, controls, testing, exceptions, complementary user-entity controls, and subservice organizations.

Examples of areas where report recipients must be aware of its limitations include:

- **Threat-landscape Coverage:** A report recipient must confirm each SOC 2 report includes the necessary controls to mitigate risks according to their expectations. The controls included in a SOC 2 are intended for organizations to address the Trust Services Criteria (TSCs), which are not aligned with the current threat landscape.

- **Quality Approach:** SOC 2 audits do not have report pre-issuance quality procedures independent from the issuing firm. Instead, the SOC 2 audit firm's peer review occurs after reports have been issued. A report recipient that intends to place significant reliance on a SOC 2 report should consider the firm's qualifications, experience, licensure, peer review status, and quality record when relying on that report.

- **Supply Chain Coverage:** SOC 2 report recipients should be aware they often will need to obtain and review separate assurance reports for each service provider utilized by their vendors to obtain necessary assurance around their outsourced services. We examined a sample of SOC 2 reports[1] and identified 100% of the reports applied the carve-out method for all subservice organizations (i.e., service providers), leaving those service providers' controls outside the SOC 2 examination.

- **Measurable Outcomes:** SOC 2 does not use a standardized numeric cybersecurity score across reports. A report recipient comparing reports must consider that two reports may have significant variability in controls, testing and results, resulting in a manual process requiring considerable judgement. This absence of standardized scoring therefore becomes a limitation for high-volume vendor comparison by report recipients.

In summary, SOC 2 is **an artifact which requires scrutiny by recipients to interpret assurance coverage.** A recipient who carefully reviews each report understanding its limitations can obtain a commensurate assurance value from their vendor's SOC 2 reports.

HITRUST'S APPROACH

HITRUST is continually innovating and improving processes to reduce the interpretation burden for TPRM teams. A key value of a HITRUST certification is when the report recipient needs a more prescriptive, comparable, and quality-controlled form of assurance.

Review Area	HITRUST Design Approach	Report Recipient Benefits
Scope	A standardized report format with scope rules that requires consistent inclusion and formatting of scope components and facilities related to the in-scope system(s).	Efficient review and comparison of in-scope system(s) across HITRUST reports.
Threat-landscape Coverage	Structured, prescriptive HITRUST requirements within each assessment. Cyber Threat Adaptive process used to evaluate and update requirements against the latest threat intelligence.	More consistent expectations and less need to infer control inclusions. A more explicit connection between the assessed requirements and current attack techniques.
Quality	Independent external assessment followed by centralized HITRUST quality assurance processes and HITRUST-issued reports for every assessment.	A common quality layer across assessors and a reduced burden on report recipients to evaluate each firm's quality process from scratch.
Supply Chain Coverage	Shared Responsibility Matrices and inheritance capabilities that allow validated controls performed by third parties to be reused in an assessment.	A structured path to represent outsourced control performance rather than relying only on vendor-management language or separate artifacts.
Measureable Outcomes	Standardized scoring, assessment outputs, and certification rules.	More consistent and efficient vendor comparison.

A well-designed report or certification can reduce duplicative work by allowing multiple report recipients to use a common body of evidence. But reuse is safe only when the artifact is fit for the decision. TPRM teams should not measure success by the percentage of vendors that supplied a report. They should measure whether the supplied evidence supports the risk decision, whether gaps are identified and supplemented, and whether the conclusion can be defended to management, regulators, customers, and auditors.

The Assurance Gap

Organizations rely on information security assurance to reduce risk. But what level of relevance and reliability do the various assurance report types provide for their recipients?

Modern enterprises operate through ecosystems. Cloud platforms, software-as-a-service providers, data processors, payment services, managed service providers, and specialized subcontractors may all participate in delivering a single customer-facing capability. The security posture of one organization is therefore increasingly dependent on the security practices of many others.

As a result, information security assurance, both internally and with vendors and suppliers, has become a core operating requirement for modern enterprises to operate securely. Third-party risk management teams require scalable ways to evaluate vendor risk, while vendors need credible ways to demonstrate trust without responding to endless questionnaires. This has resulted in a broad acceptance of various types of assurance artifacts which are often treated as interchangeable. They are not.

> WE BELIEVE THAT TODAY'S ASSURANCE PROVIDERS HAVE **A RESPONSIBILITY TO PROVIDE TRUSTWORTHY ASSURANCE** GROUNDED IN REAL-WORLD THREATS, INDEPENDENT OVERSIGHT, AND MEASURABLE OUTCOMES.
>
> **- 2026 HITRUST TRUST REPORT**

The assurance gap often arises because the artifact and the reliance decision were designed at different levels of specificity. A service auditor may perform an examination in accordance with professional standards. A certification body may audit a management system. A vendor may accurately complete a questionnaire. Yet the resulting evidence can remain insufficient for a recipient that needs to know whether a particular system, environment, control, or dependency is protected.

The gap is therefore a fit problem. It appears when the assurance report recipient assumes the label on an artifact conveys more than the underlying assessment supports. A "clean" report may cover the wrong controls. A certification may cover the enterprise management system but not the environment the customer uses. A payment-card assessment may say little about non-payment systems. A report may describe intended outcomes without independent validation. A questionnaire may be complete but self-attested and unreliable.

Where the gap appears	What the report recipient may assume	What must be verified
Scope	The report covers the vendor relationship in full.	The legal entity, product, system boundaries, locations, data, review period, and exclusions match the service(s) used by the recipient.
Threat-landscape Coverage	"Security" means a complete cybersecurity baseline.	Controls relevant to the recipient are explicitly included, implemented, and validated.
Quality	A recognizable report label implies consistent audit rigor.	The practitioner is qualified and independent, testing is sufficient, and the engagement has been subject to credible quality management and review.
Supply Chain Coverage	The direct vendor's artifact covers the full service chain.	Service providers (e.g. cloud providers) and shared responsibilities are included or separately assessed (when excluded).
Measureable Outcomes	Two "clean" artifacts indicate similar security maturity.	Controls, exceptions, scoring, and conclusion logic are sufficiently standardized to support comparison through measured outcomes.

The assurance gap matters because organizations rely on assurance artifacts to approve a vendor, reduce questionnaire depth, set monitoring frequency, accept residual risk, satisfy a contractual obligation, or demonstrate oversight. When the artifact is treated as stronger or broader than it is, the downstream decision becomes less defensible even if the artifact itself is valid.

The remedy is to apply **a consistent reliance model that makes assumptions explicit and validates the evidence is sufficient for the decision at hand.**

The Assurance Market

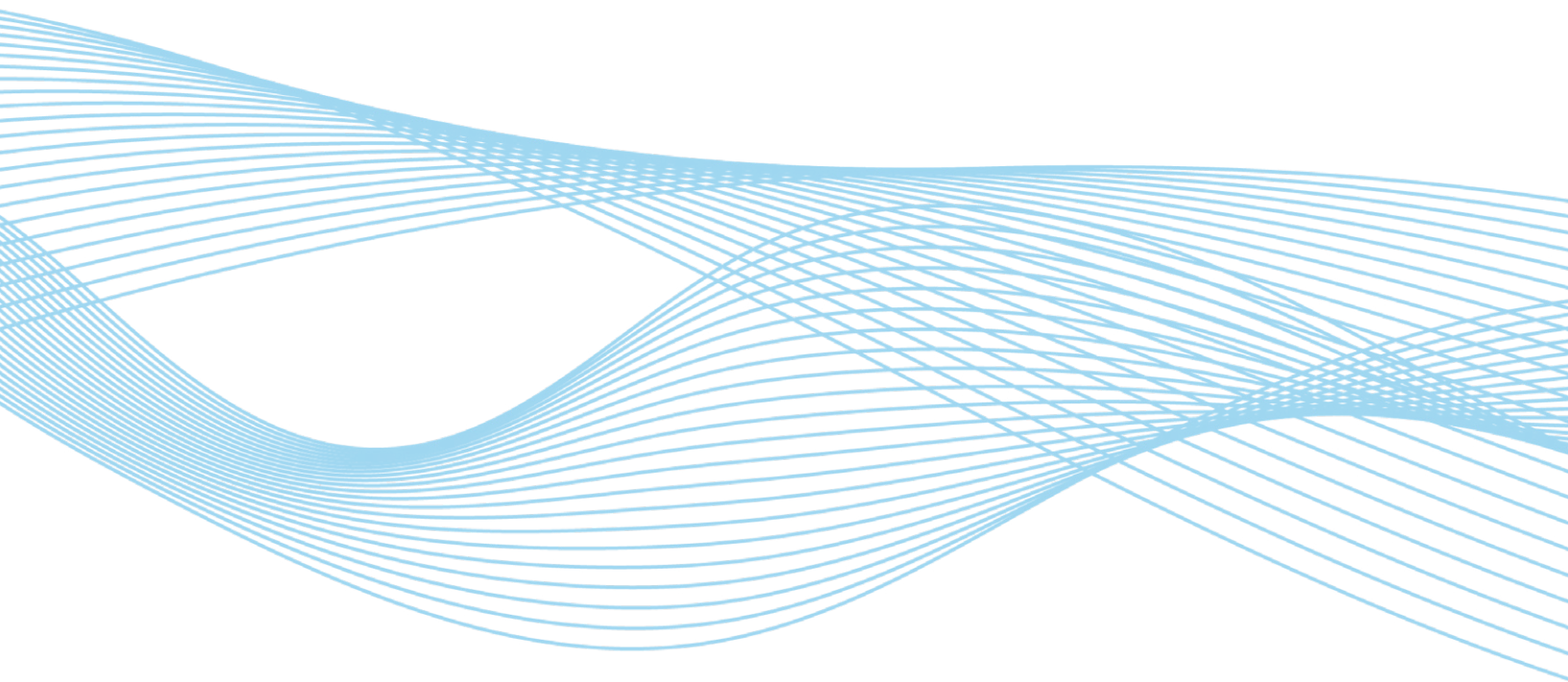
Information security assurance is a market of different instruments. Some mechanisms establish management system requirements. Some prescribe control requirements. Some provide an auditor's opinion on management-defined controls. Some offer a common taxonomy for organizing risk. Some are self-assessments or information requests. Comparing them requires first understanding what each one was designed to do.

Mechanism	Primary Purpose	Nature of Approach	Key Reliance Caution
HITRUST	Validated assessment and certification against a structured set of HITRUST CSF requirements, with assessment depth selected by risk and use case.	External assessor testing, standardized scoring, centralized HITRUST quality review, and HITRUST-issued reporting/certification.	Assessment type and scope still matter. Comparability is strongest when the same assessment type and similar scope are used.
SOC 2	Provide users with information about a service organization's system and controls relevant to the Trust Services Criteria.	Management assertion and system description examined by an independent CPA; Type 2 includes operating-effectiveness testing over a period.	Controls, criteria, system boundaries, test approaches, exceptions, and subservice treatment vary. Detailed report review is essential.
ISO/IEC 27001	Establish and certify an information security management system (ISMS) that manages information-security risk.	Certification by an independent certification body; the certificate, scope statement, and Statement of Applicability are central reliance documents.	A certificate confirms conformity of the ISMS within scope. The organization determines its controls, and may exclude ISO-suggested controls (Annex A) with justification. Verify scope and certification-body accreditation.
NIST CSF	Provide a taxonomy of high-level cybersecurity outcomes for managing and communicating risk.	Profiles, tiers, mappings, and implementation evidence developed by the organization or assessor. NIST CSF 2.0 is a framework, not a certification.	Use of the framework alone does not establish implementation, operating effectiveness, independence, or assurance level.
PCI DSS	Protect account data within the payment-card ecosystem through prescriptive requirements and defined validation methods.	Self-assessment or independent assessment/reporting depending on entity type and validation obligations; the current standard is PCI DSS v4.0.1.	Strong evidence for the cardholder-data environment does not automatically address enterprise-wide cybersecurity risk outside that scope.
Questionnaires	Collect decision-specific information from a vendor, often to fill gaps left by reusable artifacts.	Usually management responses, sometimes supported by evidence or validation; may be standardized or bespoke.	Self-attestation, inconsistent wording, stale responses, and duplicated evidence requests can reduce reliability and comparability unless the process is governed.

This comparison shows why “which one is best?” is usually the wrong question. A payment processor may need PCI DSS evidence because the decision concerns cardholder data. An enterprise may use NIST CSF to organize its cybersecurity program and another mechanism to obtain independent assurance. A report recipient may accept SOC 2 for one vendor and require a more prescriptive certification for another based on inherent risk.

The correct mechanism is the one that provides **sufficient, current, and credible** evidence for the decision, at a cost and level of effort proportionate to the risk. In many cases, the best answer is a reusable baseline report or certification, targeted supplemental evidence, and ongoing monitoring of change.

This report examines SOC 2 in greater depth since it is one of the most widely accepted assurance mechanisms, evaluating several of the previously identified areas where assurance gaps may exist.



SOC 2: What It Is, and What It Is Not

SOC 2 is part of the AICPA's System and Organization Controls reporting suite. The AICPA describes SOC 2 as an assertion-based examination of a service organization's description of its system and its controls relevant to security, availability, processing integrity, confidentiality, or privacy. Customers and business partners request these reports because they need information about the design, operation, and effectiveness of controls used to provide outsourced services.

In a SOC 2 engagement, management defines the system, prepares the system description, identifies the applicable Trust Services Criteria (TSC), describes the controls designed to meet those criteria, and makes an assertion. An independent CPA performs the examination and expresses an opinion.

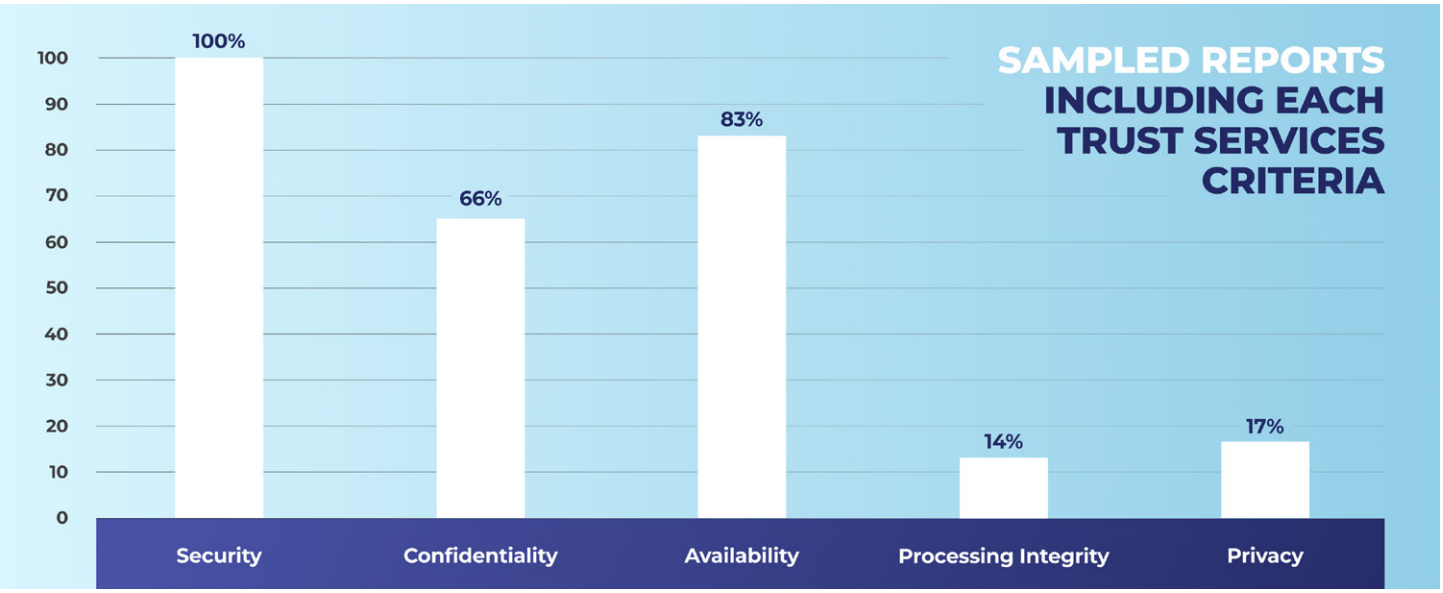
This structure can be useful if the recipient expends the effort to interpret each report individually. A strong SOC 2 Type 2 report[2] can provide detailed descriptions of the service, control environment, tests performed, examination period, and exceptions identified. It can help recipients understand how the vendor operates and can support targeted follow-up. It also gives organizations flexibility to design controls that fit their technologies, risks, and operating models rather than forcing every service into an identical implementation pattern.

That same flexibility means the reader must do more interpretive work. The Trust Services Criteria are criteria for evaluating controls, not a universal catalog of required cybersecurity protections. Management-defined controls, system boundaries, complementary user-entity controls, and treatment of subservice organizations can vary significantly across multiple SOC 2 reports. Two reports bearing the same label can therefore provide variable levels of information security assurance. In the following sections we will review examples of SOC 2 reliance limitations that a report recipient may encounter.

SOC 2: Threat-landscape Coverage

The Trust Services Criteria are built around five categories: Security, Availability, Processing Integrity, Confidentiality, Privacy. When an organization performs a SOC 2 they must address the common criteria available in the Security category, and they can choose whether they include any (or none) of the remaining four categories.

In this report we examined a sample of 103 SOC 2 reports issued across 37 unique audit firms. We noted that only 4% (4 reports) included all five TSC categories with the majority including Security and Availability.



Sample Analysis

MITRE ATT&CK[3] is widely regarded as a trusted, leading framework for understanding attacker behavior because of how it is built, maintained, and used across the cybersecurity ecosystem. In our SOC 2 analysis we identified that even if an organization selected all five categories for their SOC 2 report, **the criteria within the TSCs only map to 67% of the attack methods within MITRE ATT&CK.** An organization may choose to include additional controls in their SOC 2 (providing increased ATT&CK coverage), but this is not required to meet SOC 2 coverage criteria.

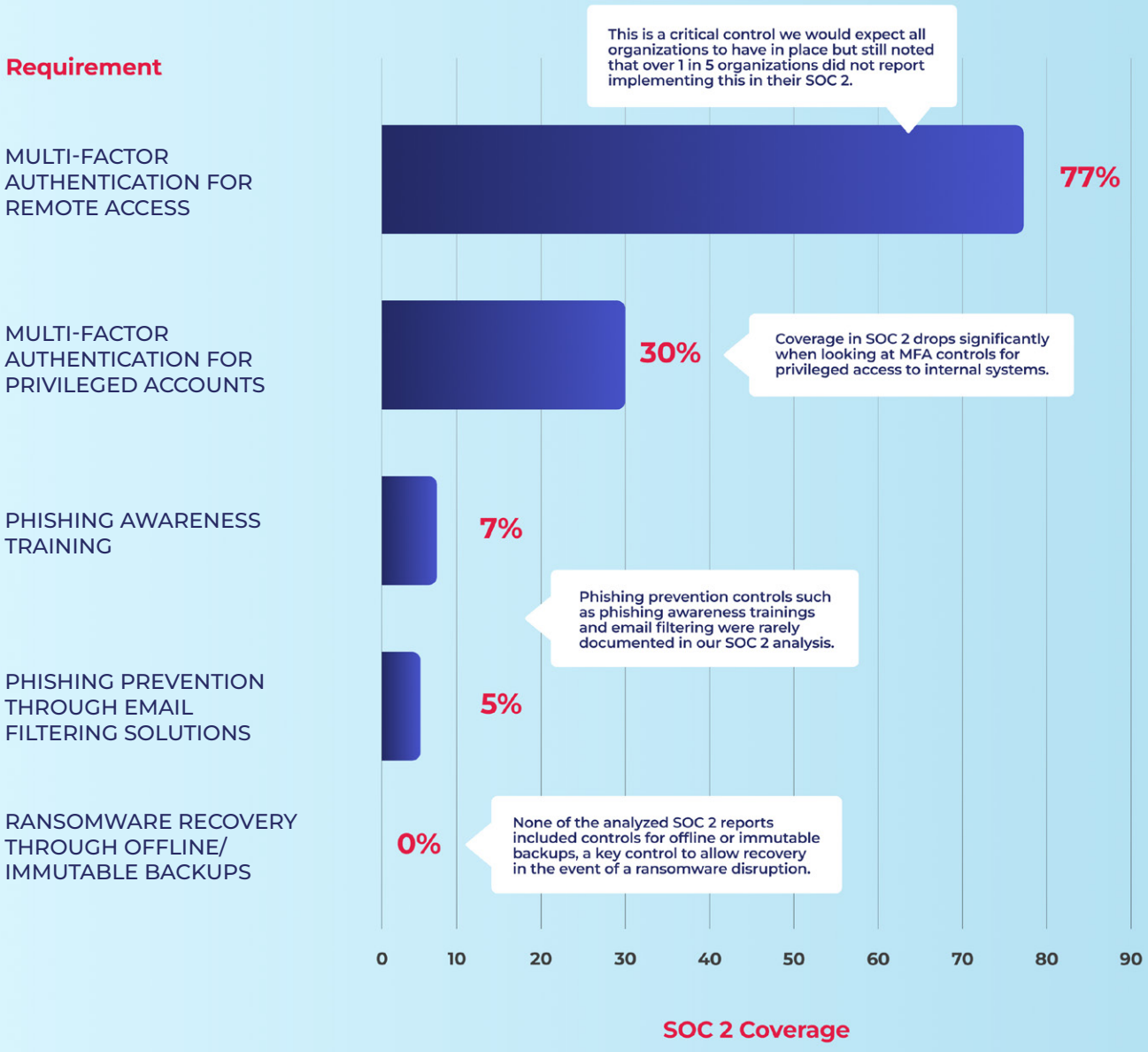
SOC 2 aims to deliver broad applicability using the TSCs, offering organizations the flexibility to address those points of focus based on their specific risks and identified controls. However, this also causes gaps in coverage when their implemented controls are not based on current threat intelligence. This places the burden on both the organization and the report recipients **to ensure the correct controls have been defined to address the necessary threats.**

We also examined this sample of SOC 2 reports to understand if common threat actions were being addressed through organization-defined controls within the reports. Our analysis focused on essential requirements within all HITRUST assessments which mitigate ransomware, phishing, and credential compromise attack techniques.

2026 Top Threat Action

The Verizon 2026 Data Breach Investigations Report (DBIR) **reported Ransomware as the most common action** attackers are performing in breaches (48% of reported breaches[4]), with web applications and email being the most frequently targeted assets, involved in 54% and 30% of breaches respectively[5], demonstrating the importance of securing those assets.

SOC 2 THREAT COVERAGE SUMMARY[6]



ATTACK TECHNIQUE: CREDENTIAL COMPROMISE

"You should stop postponing that MFA rollout in your organization because credentials are an integral part of the threat actor's toolkit."

- Verizon 2026 Data Breach Investigations Report (DBIR)[7]

Requirement	Sampled SOC 2 Coverage: 24%
MULTI-FACTOR AUTHENTICATION FOR REMOTE ACCESS[8]	In the sampled SOC 2 reports, we identified that **77%** of the reports stated that multi-factor authentication (MFA) controls were required for remote access into the in-scope environment but only **30%** included controls requiring MFA for privileged access to the in-scope system(s). Combined, only **24%** of the SOC 2 reports included controls expecting MFA for both remote access and privileged access.
MULTI-FACTOR AUTHENTICATION FOR PRIVILEGED ACCOUNTS[9]	

We don't believe anyone today would argue that multi-factor authentication (MFA) is one of the most important controls an organization can implement. In fact, HITRUST threat intelligence indicates that MFA is a mitigation strategy for 19 different attack techniques, with MFA for privileged access mitigating 26% of those techniques. However, our SOC 2 analysis indicates that most organizations are only obtaining assurance around their deployment of MFA to the remote access layer. HITRUST's threat intelligence shows that including MFA for internal privileged access further helps prevent adversaries from leveraging credentials once inside the network boundary.

ATTACK TECHNIQUE: PHISHING

"When we're looking at data from email security gateways, we see similar breakdowns, with 80% of the attacks blocked being plain phishing, 10% being emails with malware, 5% being attempts of getting the victim to call back to the attacker and 3% consisting of Business Email Compromise-style attacks."

- Verizon 2026 Data Breach Investigations Report (DBIR)[10]

Requirement	Sampled SOC 2 Coverage: 1%
PHISHING AWARENESS TRAINING[11]	In the sampled SOC 2 reports, **7%** included a control for dedicated phishing trainings or phishing simulations. In the sampled SOC 2 reports, **5%** included a prescriptive control requiring an email filtering solution to block suspicious emails and unnecessary file types before they reach inboxes. Combined, only **1%** of the SOC 2 reports included controls which mapped to both of these requirements intended to address phishing (and, by extension, malware) threats (11% had either of the controls represented).
PHISHING PREVENTION THROUGH EMAIL FILTERING SOLUTIONS[12]	

We noted that most of the analyzed SOC 2 reports included the performance of general security awareness trainings[13]. However, organizations rarely defined the performance of specific phishing trainings or simulations as a control in their SOC 2 report.

As human error has consistently been a leading breach cause[14] and phishing remains the initial access vector for 16% of all breaches[15], it is important for organizations to consistently reinforce employee vigilance against the potential threat of phishing. The exclusion of both preventive controls from 89% of SOC 2 reports is a clear example of how broad criteria can lead to a failure for organizations to implement and/or validate those controls necessary for breach protection.

ATTACK TECHNIQUE: RANSOMWARE

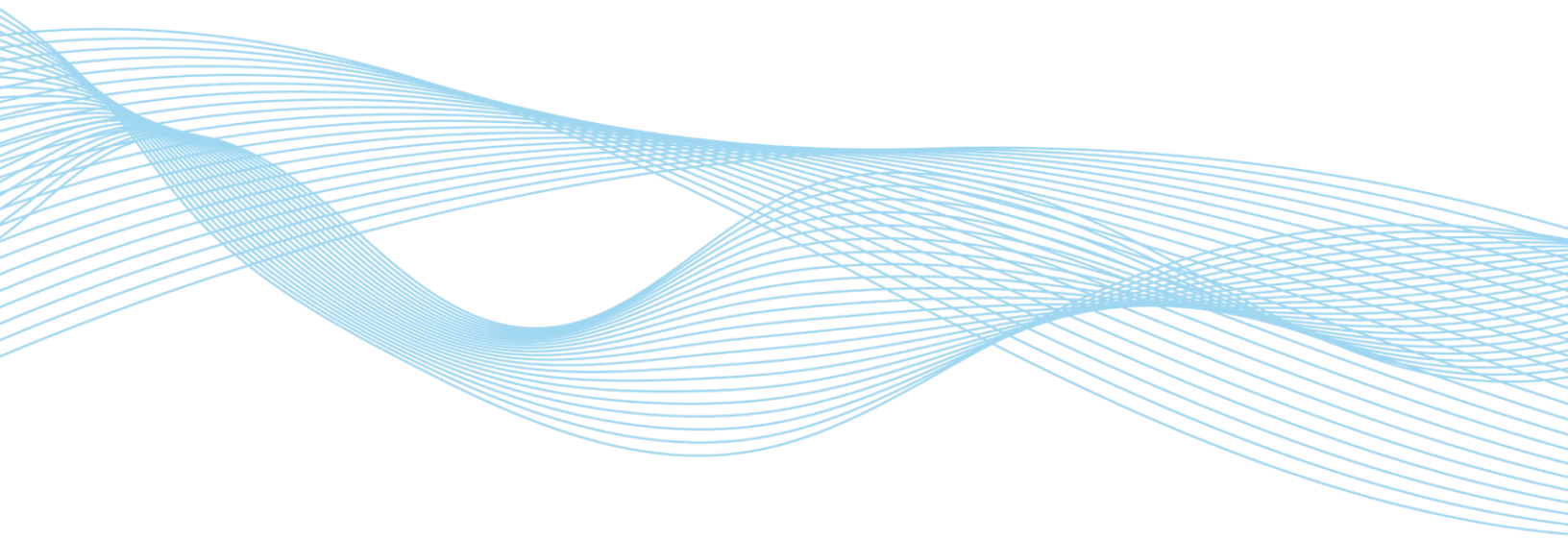
" ...Ransomware is still the yoga pants of cybersecurity— ubiquitous, stubbornly popular and appearing in unexpected places near you. Nearly half (48%) of breaches in this report feature Ransomware somewhere in the attack chain."

- Verizon 2026 Data Breach Investigations Report (DBIR)[16]

Requirement	**Sampled SOC 2 Coverage: 0%**
RANSOMWARE RECOVERY THROUGH OFFLINE/ IMMUTABLE BACKUPS[17]	In our analysis, **0%** of the sampled SOC 2 reports included an organizational control to maintain offline or immutable backups of their data. This is considered a key control to allow organizations to restore their prior environment without being subject to the demands of the attacker.

A common misconception is that smaller organizations are less at risk of Ransomware due to being a less valuable target. However, according to the Verizon 2026 DBIR[18] *"Of the Ransomware cases where we have information on the organization size, we found that about 96% of Ransomware victims were small-and medium-sized businesses."* For smaller businesses using CSPs, many cloud hosting providers include the ability to make backups immutable with limited effort or organization expense.

These findings most clearly illustrate the assurance gap. The absence of a control from a SOC 2 report does not prove the control is absent from the environment. It does, however, mean a report recipient cannot use the report to confirm the control. If the control is material to the decision, the recipient must request supplemental evidence or use another assurance mechanism which prescribes and tests the control. This **introduces delays into the TPRM process that can cause friction** with other teams in the organization.



SOC 2: Quality Approach

Assurance processes must have the necessary mechanisms to report *reliable* results without the ability to circumvent their built-in quality structure. This reliability can be demonstrated through the assurance provider's processes to report accurate results.

> "PROMISES OF 'FAST AND EASY' **THREATEN SOC CREDIBILITY."**
>
> **- JOURNAL OF ACCOUNTANCY, FEBRUARY 2026**

Under the AICPA's SOC 2 program, reports are produced and distributed by individual CPA firms. The AICPA requires those firms to implement Quality Management Standards to identify, assess, and manage risks related to SOC 2 (and other audit) services.

While the Quality Management Standards include certain required quality procedures within each audit firm, there are no pre-report issuance quality procedures separate and independent from the issuing firm. The AICPA typically has no visibility into the underlying assessment performed and does not review SOC 2 reports prior to their issuance. This can result in unaddressed quality and consistency issues in those reports due to lack of centralized oversight or misaligned incentives.

The SOC 2 "Template Audit" Scheme

In early 2026, there were discussions around the potential issuance of fraudulent SOC 2 reports. In this scheme, an automated compliance platform generated almost identical reports across multiple organizations. These reports were allegedly "rubber-stamped" by partner audit firms with no actual verification of the companies' security controls.

While we have no perspective on the factual nature of the allegations, the amount of commercial pressure to obtain SOC 2 quickly along with the emergence of automation tools and accelerated audit offerings has contributed to this possibility. This pressure has produced incentives on the automated compliance platforms and audit firms to cut corners on quality without immediate repercussions *since there is no independent and centralized body performing quality reviews of the work or report prior to issuance.*

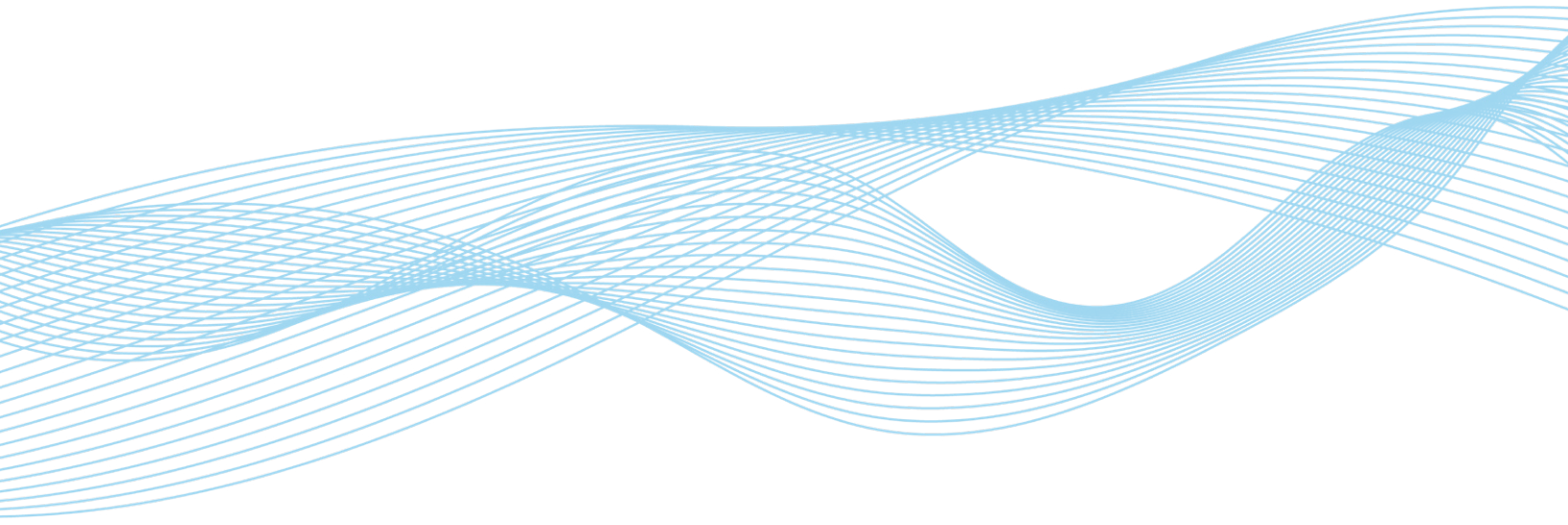
We believe the majority of audit firms performing SOC 2 reports are acting in good faith with their SOC 2 report issuances. However, these types of situations highlight the importance for a report recipient to validate the audit firm's background for each SOC 2 report.

Enforcement of the AICPA Quality Management Standards is primarily through the AICPA's peer review program. This quality process relies on another CPA firm performing sample-based audits of that firm's completed SOC 2 assessments. Recipients of a SOC 2 should be aware of potential limitations and risks of this quality approach:

- Peer reviews are performed post-issuance so the results may not result in corrections to previously issued SOC 2 reports.
- Firms are allowed to select the audit firm performing the peer review, which could introduce bias into the process.
- Peer reviews are only required to be performed once every three years which can result in a high volume of SOC 2 reports being issued before quality concerns can be identified.
- The sample-based audit approach means that only a select number of SOC 2 reports are reviewed for each firm.

This is not an assertion that the SOC 2's decentralized quality model is inherently unreliable. However, a SOC 2 (or other decentralized assurance report) recipient should evaluate the assurance provider as part of evaluating the report. A report recipient that intends to place significant reliance on a SOC 2 report should consider the firm's qualifications, experience, licensure, peer review status, and quality record when relying on that report.

The best practice is that quality must be visible enough to support the level of reliance. The higher the consequence of a wrong vendor decision, the stronger the need for independent testing, qualified practitioners, transparent methods, and quality review beyond the individual preparer.



SOC 2: Supply Chain Coverage

Adversaries have identified that security weaknesses in an organization's third-parties can provide a path for adversaries into the target organization[19]. Despite rising supply chain attacks, service providers are necessary components for efficient and strategic operations. As a result, assurance mechanisms must address those risk areas managed by an organization's third-parties.

Even with intensifying supply-chain attacks, many assurance mechanisms, including SOC 2, do not have an efficient path for service provider inclusion in their reports. Instead, SOC 2 reports typically rely on organizational controls around vendor oversight and third-party agreements.

SOC 2 provides defined methods for addressing subservice organizations (i.e., service providers). Under the inclusive method, the relevant controls of the subservice organization are included in the system description and examination. Under the carve-out method, the controls are excluded, and the report describes the nature of the services and the service organization's controls for monitoring the subservice organization. Carve-out is a scope choice that shifts additional review responsibility to the report user.

Sample Analysis

During our analysis of over 100 SOC 2 reports, we identified that while 80.4% of organizations used at least one subservice organization, 100% of those reports carved-out the subservice organization. As a result, ***none* of those reports covered or tested those key service providers as part of the assessment.**

The SOC 2 approach does not necessarily mean the vendors are failing to manage their service providers. Instead, SOC 2 report recipients should be aware that **they often will need to obtain and review separate assurance reports for each service provider** utilized by their vendors to obtain necessary assurance around their outsourced services.

SOC 2: Measurable Outcomes

Assurance conclusions are often compressed into labels such as: “unqualified opinion”, “certified”, “compliant”, or “questionnaire complete”. Those labels are meaningful within their own programs, but they rarely communicate enough detail to compare vendors without further analysis.

In SOC 2, an “unqualified” opinion means the service auditor did not identify control exceptions material enough to modify the opinion based on the applicable criteria and report. It does not mean that every test had no exceptions. A report can contain individual deviations that the auditor evaluates as not material to the overall opinion (without a corresponding rationale from the audit firm). The reader must review the tests and results, understand the significance of exceptions, and consider management responses and remediation evidence where available.

Sample Analysis

Within our examination of 103 SOC 2 reports, we identified:

- Each of the reports contained a clean (unqualified) opinion, but **40% of the SOC 2 reports contained one or more exceptions** which needed to be reviewed.
- Of those SOC 2 reports with exceptions, there was **an average of 3.6 exceptions** per SOC 2 report.

This does not suggest the opinions were inappropriate, but it demonstrates why “clean opinion” should not be translated into “no exceptions” or “same maturity as another clean report.”

SOC 2 does not use a standardized numeric cybersecurity score across reports. Control sets and scopes vary, exception summaries and management responses may differ, and two audit firms may present detail differently. A report recipient can still compare reports, but the process is manual and requires judgement. **This absence of a universal score therefore becomes a limitation for high-volume vendor comparison by report recipients.**

Five Questions for Evaluating Assurance

Our examination of SOC 2 is not intended to position it as a defective mechanism, rather an artifact which requires scrutiny by its recipients. A recipient who carefully reviews each report may obtain significant value. However, **recipients that simply record "SOC 2: yes" in a table may obtain less assurance than they believe.**

Each assurance mechanism can be evaluated by its recipient through similar questions. These questions can be applied to HITRUST, SOC 2, ISO 27001, PCI DSS, a NIST-based assessment, a questionnaire, or a combination of artifacts. The objective is to move the review from label recognition to evidence sufficiency.

Review Area	Questions	Common Warning Signs
Scope	Does the entity, service, environment, data, geography, period, and dependency model match the relationship?	The artifact covers the parent company but not the product; scope language is generic; the service was acquired after the review period; key locations, environments, or service providers are excluded.
Threat-landscape Coverage	Are the controls required by the threat-intelligence model, regulation, contract, and/or risk tier explicitly included and tested?	"Security" is treated as a complete baseline; controls are described at a high level; key controls are optional or absent; mappings substitute for implementation evidence.
Quality	Is the preparer qualified and independent? What quality management, peer review, accreditation, or centralized review applies?	Unknown practitioner; minimal testing detail; no way to verify accreditation, licensure, peer review, or quality process; the same party designs, tests, and approves without safeguards.
Supply Chain Coverage	Which subservice organizations perform critical controls? Are they inclusive, carved out, inherited, or separately assessed?	Exclusion of service providers in scope; Controls not applicable because they are performed by service provider.
Measureable Outcomes	Can this result be fairly compared with other vendors, or must the team normalize scope, controls, and scoring?	Same label but different criteria and scopes; no exception summary; no standardized score; differing auditor methods; material exclusions hidden in narrative detail.

These questions are a way to identify what an assurance artifact supports, what it does not support, and what supplemental work is required. A lower-risk vendor may warrant a lighter answer. A critical processor of regulated data may require narrow scope precision, prescriptive controls, independent validation, and ongoing monitoring. **The level of reliance should rise only when the evidence quality rises with it.**

The HITRUST Approach

HITRUST has continuously innovated in the assurance process to support a more efficient review by report recipients while also reducing those recipients' risk. These processes have been summarized below, while additional detail on each process can be found within the 2026 HITRUST Trust Report.

THREAT-LANDSCAPE COVERAGE

HITRUST uses the MITRE ATT&CK framework to identify the methods that attackers use to initiate and operate a cyber attack. The HITRUST CSF is built around a prescriptive set of requirement statements and mapped to those methods, creating a control framework based on real-world attack scenarios. For each HITRUST assessment type, we identified the following:

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

HITRUST also continually updates those requirements using our Cyber Threat Adaptive (CTA) process. CTA is explicitly designed to keep requirements "highly relevant and effective" against emerging risk.

HITRUST's Cyber Threat Adaptive Approach

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

For our latest analysis, see: https://hitrustalliance.net/cyber-threat-adaptive

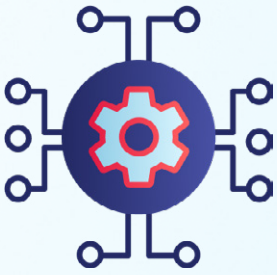
QUALITY APPROACH

HITRUST separates assessment fieldwork from centralized quality review and report issuance. HITRUST assessment work is performed (and quality-reviewed) by an independent group of external assessors and then submitted to HITRUST to undergo another detailed, independent quality review process prior to report and certification issuance. The benefit is a common quality layer across external assessors and a more standardized report-issuance process.

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

SUPPLY CHAIN COVERAGE

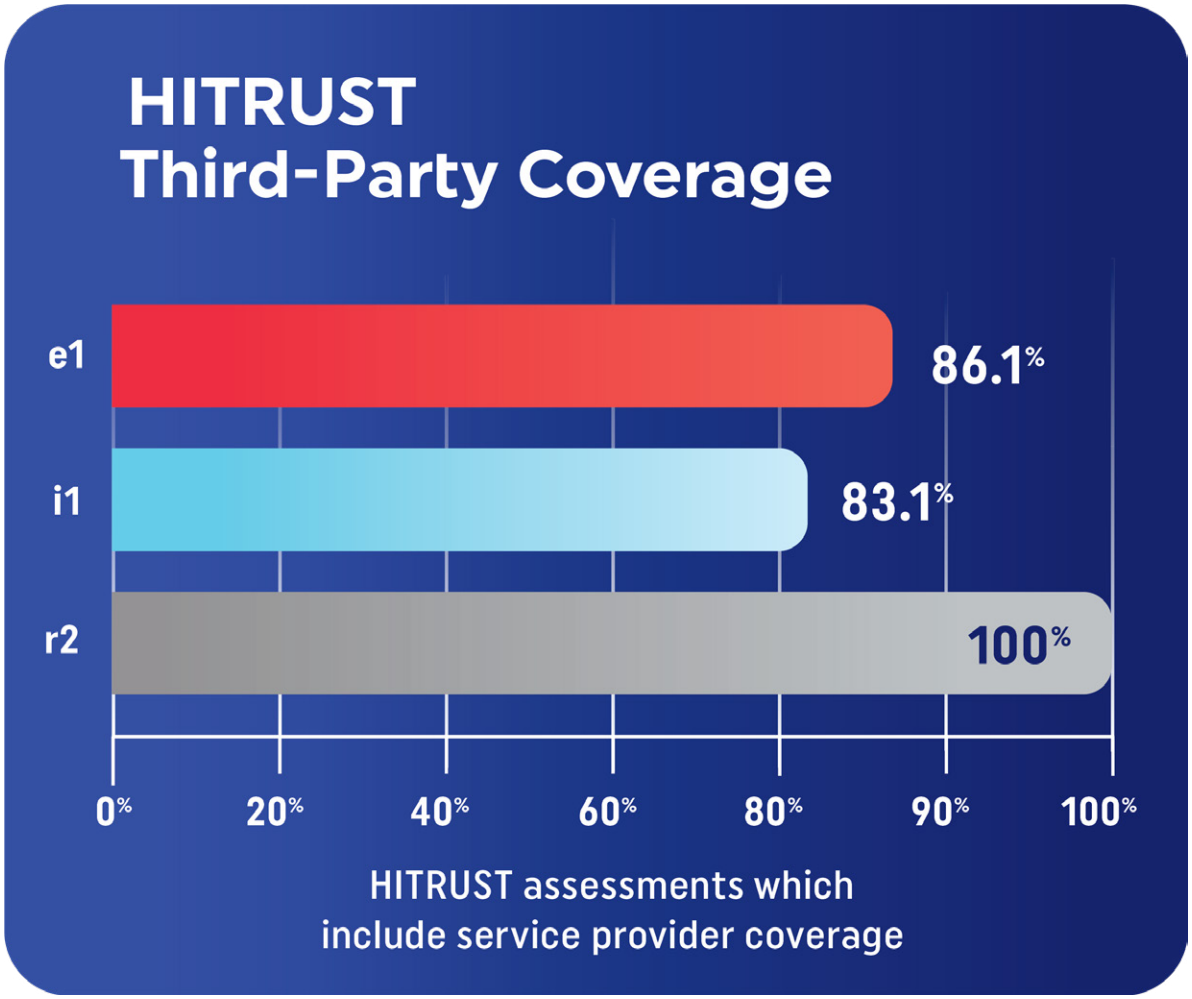
HITRUST provides a simple and efficient path for organizations to include the security results of their service providers in a HITRUST assessment. To assist organizations with identifying those requirements which should be scored for service providers, HITRUST offers shared responsibility matrices (SRMs) along with simplifying the service provider assessment process through its *Inheritance functionality*. Inheritance allows HITRUST assessments to incorporate scoring from other HITRUST-certified organizations.



Inheritance Functionality

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

As a result of the efficient approach provided by HITRUST, **over 80% of HITRUST certifications,** including 100% of r2 certifications, address the organization's service providers.

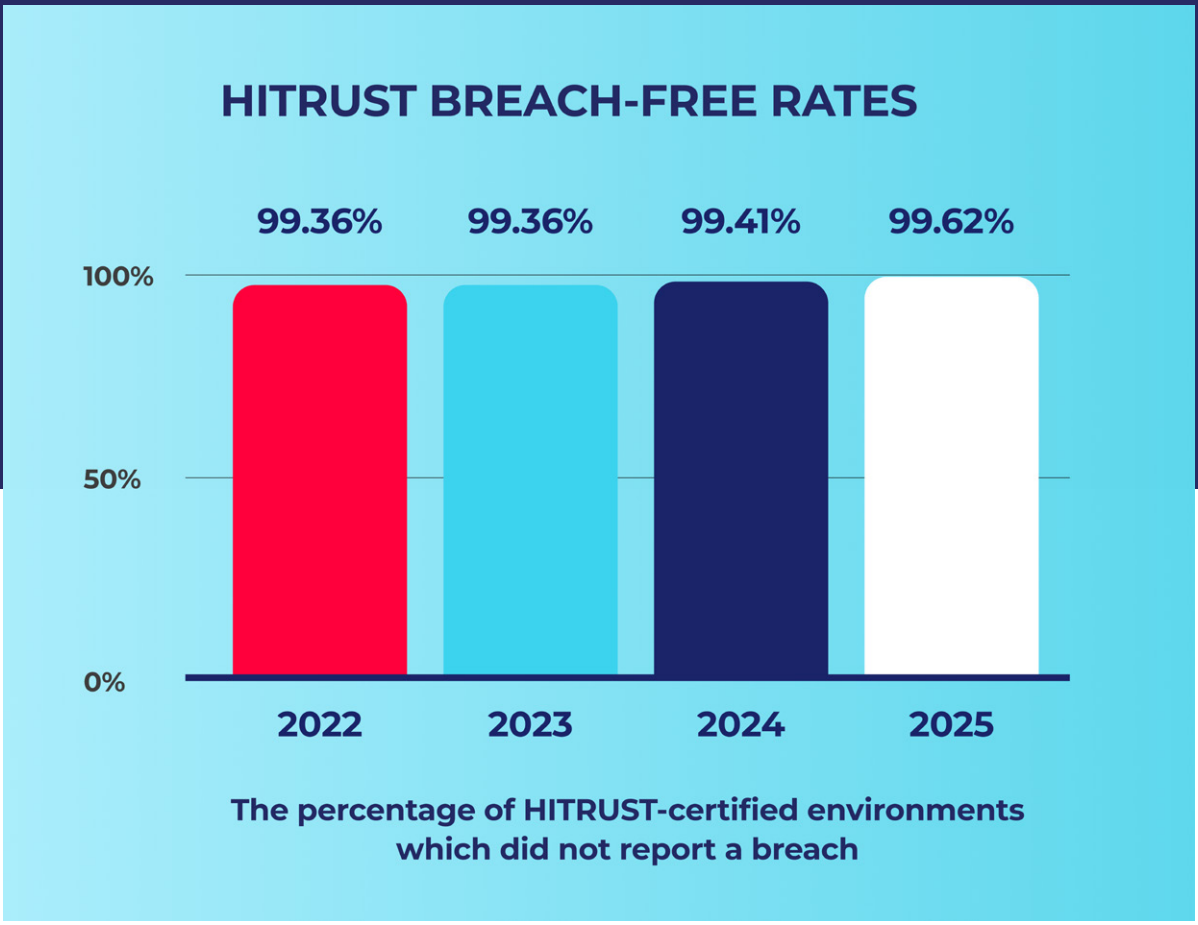


MEASURABLE OUTCOMES

Organizations undergoing a HITRUST assessment must obtain a specific score to achieve HITRUST certification. The scoring in a HITRUST assessment uses an innovative PRISMA-based control maturity and scoring model. Unlike other assurance providers that rely on binary pass-or-fail determinations, the HITRUST scoring model reflects modern risk management by recognizing varying degrees of control maturity and effectiveness. This more nuanced, risk-based approach provides organizations with a clear, actionable understanding of their security posture.

Even if they obtain the scores necessary for certification, organizations may have areas where they can improve their security postures. These requirements are recorded within each HITRUST certification report requiring the organization to document a Corrective Action Plan (CAP) to remediate the deficiency. Within the 2026 HITRUST Trust Report, we highlighted how organizations have lowered their average number of CAPs across all HITRUST assessment types on a year-over-year basis reflecting **continuous improvement** in security posture.

Review Area	HITRUST Design Approach	Report Recipient Benefits
Scope	A standardized report format with scope rules that requires consistent inclusion and presentation of scope components and facilities related to the in-scope system(s).	Efficient review and comparison of in-scope system(s) across HITRUST reports.
Threat-landscape Coverage	Structured, prescriptive HITRUST requirements within each assessment. Cyber Threat Adaptive process used to evaluate and update requirements against the latest threat intelligence.	More consistent expectations and less need to infer control inclusions. A more explicit connection between the assessed requirements and current attack techniques.
Quality	Independent external assessment followed by centralized HITRUST quality assurance processes and HITRUST-issued reports for every assessment.	A common quality layer across assessors and a reduced burden on report recipients to evaluate each firm's quality process from scratch.
Supply Chain Coverage	Shared Responsibility Matrices and inheritance capabilities that allow validated controls performed by third parties to be reused in an assessment.	A structured path to represent outsourced control performance rather than relying only on vendor-management language or separate artifacts.
Measureable Outcomes	Standardized scoring, assessment outputs, and certification achievement rules.	More consistent and efficient vendor comparison.



The strength of the HITRUST program, which has allowed us to build Trust throughout the HITRUST community, is in the design of these assurance processes to create relevant and reliable assurances. This approach has resulted in a multi-year trend of low breach rates, **including 99.62% of HITRUST-certified environments not reporting a breach in 2025.**

Closing Perspective

An assurance artifact is evidence for a risk decision. The degree of reliance depends on whether the organization understands what the evidence proves, what it leaves open, and how those gaps are addressed. Reliance can fail when a recipient assumes that a report covers the full service, includes a complete threat baseline, extends to downstream providers, reflects current conditions, or supports direct vendor comparison without detailed review.

SOC 2 should be treated as a detailed, assertion-based attestation report, rather than elevated into a universal cybersecurity certification. ISO 27001 should be understood as certification of an information security management system within a defined scope. NIST CSF should be used as a risk-management framework, not as proof of implementation by itself. PCI DSS should be relied upon for its payment-card purpose and scope. Questionnaires should be used to fill decision-specific gaps rather than recreate the entire baseline.

Across all assurance mechanisms, the same five questions should be investigated by the report recipient:

- Does the scope cover the provided service?
- Is the assurance dynamic to expected risks and threats?
- Who prepared and quality reviewed the work?
- What service providers are included and are they assessed?
- Can two reports be measurably compared?

HITRUST is designed to reduce assurance friction by standardizing requirements, incorporating threat intelligence, applying external validation and centralized quality review, supporting inheritance and shared responsibility, and producing structured results that are easier to reuse and compare. These unique assurance processes are intended to provide a more consistent option when the report recipient needs a higher degree of confidence and lower interpretation burden.

Third-party risk management teams need scalable assurance mechanisms that can be compared across vendors. HITRUST can therefore be beneficial for third-party risk management programs that require greater consistency across large risk-tiered vendor populations than a flexible or self-attested mechanism can provide alone.

Footnotes

[1] Our detailed SOC 2 analysis in this report included an examination of 103 SOC 2 reports issued across 37 unique audit firms.
[2] Analysis in this report focuses on "Type 2" SOC 2 reports. A SOC 2 Type 1 report provides an independent opinion on whether controls are suitably designed as of a specified date, whereas a SOC 2 Type 2 report provides an opinion on both the suitability of control design and the operating effectiveness of those controls throughout a defined examination period.
[3] https://attack.mitre.org
[4] http://verizon.com/dbir, page 29
[5] http://verizon.com/dbir, page 33
[6] Our analysis of 103 SOC 2 reports inspected for the key controls expected by each HITRUST requirement statement within the corresponding SOC 2 report. The percentages may not reflect the actual rate of companies who have implemented these controls, as they only reflect the amount of companies who have specified the control implementation within the sampled SOC 2 reports.
[7] http://verizon.com/dbir, page 16
[8] HITRUST requirement 11.01q1System.4: The organization requires multi-factor authentication for access to non-privileged accounts from remote networks (including accounts in Web applications and in remote access solutions such as VPNs).
[9] HITRUST requirement 11.01q1System.3: The organization requires multi-factor authentication for network and local access to privileged accounts.
[10] http://verizon.com/dbir, page 48
[11] HITRUST requirement 13.02e1Organizational.6: Dedicated phishing awareness training is developed as part of the organization's onboarding program, is documented and tracked, and includes the recognition and reporting of potential phishing attempts.
[12] HITRUST requirement 09.09v1Organizational.7: The organization uses an email filtering solution to recognize and block suspicious emails and unnecessary file types before they reach employee inboxes.
[13] While SOC 2 includes security awareness training as a point of focus under CC2.2, organizations are not required to explicitly address every point of focus in a SOC 2 audit.
[14] The Verizon 2026 DBIR (http://verizon.com/dbir, page 12) reported that 62% of security breaches involved a human element.
[15] http://verizon.com/dbir, page 12
[16] http://verizon.com/dbir, page 29
[17] HITRUST requirement 16.09l1Organizational.4: The organization maintains offline and/or immutable backups of data.
[18] http://verizon.com/dbir, page 98
[19] The Verizon 2026 DBIR (http://verizon.com/dbir) reported that "breaches with third-party involvement have increased by 60% from last year's dataset, reaching 48% of total breaches.", page 11