HITRUST

How Do I Know if an Assurance Report is Rely-Able?

Given evolving cyber threats; expanding international, federal, and state privacy and security compliance requirements; growing risks associated with data management; new business models that require access to more data by more parties; and the increasing, devastating impacts from data breaches, there is broad recognition that information risk and compliance management programs are crucial in today's business environment and that appropriate assurances about these programs must be demonstrated. Organizations must not only provide assurances to internal stakeholders such as internal audit, executive management, and corporate boards about the state of their information risk and compliance programs, but also to external stakeholders such as regulators, business partners, customers, and other third parties. A strong information risk and compliance program can also be an important market differentiator, as it is a key deciding factor when evaluating vendor relationships, equity investments, and strategic partnerships.

In today's precarious threat landscape[1], the ability to provide assurances that sensitive data is being responsibly managed and adequately protected is no longer a nicety, but a necessity.

The need to be able to understand and ultimately rely on the assurances provided by an organization, usually in the form of an information security and privacy control assessment report, is extremely important. Unfortunately, the number of competing assessment and reporting options in the marketplace can make selecting the right approach challenging for many organizations.

So, how does one decide on the right approach?

Since the objective of an assessment report is to provide 'rely-able' information about an organization's ability to safeguard information and meet its compliance obligations, the report's 'rely-ability' should be the deciding factor. Given the number of breaches that have and continue to occur in organizations purported to have had appropriate controls in place, this need for 'rely-ability' cannot be overstated.

What key areas should be considered when evaluating a control assessment and reporting option?

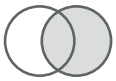
There are three key areas one should address. The first area involves the controls themselves, as they must be comprehensive in breadth and depth to ensure all reasonably anticipated threats for the applicable contexts are addressed, risks are managed appropriately, and compliance requirements are met. The second focuses on the implementation of the controls, as they should be fully implemented, monitored, and managed to ensure they operate and will continue to operate as intended. And the third area involves the trustworthiness of the information provided about the first and second areas, which generally involves considerations around the independence and overall quality of the practitioners, professional services firms, and assessment methods employed.

HITRUST has spent the last 12 years architecting and implementing a comprehensive and fully integrated approach to information risk management and compliance assessment and reporting that provides a level of transparency, scalability, consistency, accuracy, integrity, and efficiency simply not obtainable through other approaches. HITRUST's unique and comprehensive approach to information risk management and compliance—*The HITRUST Approach*—addresses all of these criteria to provide the most robust assurance option available.

What criteria must be considered when evaluating an option's 'rely-ability'?

While there are many criteria one could consider when evaluating the 'rely-ability' of a control assessment and reporting option, there are six that are key: *transparency, scalability, consistency, accuracy, integrity, and efficiency.*

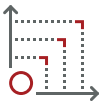
Transparency - Are the controls incorporated and the assessment approach utilized, including its evaluation and scoring model, open and transparent to all stakeholders? More specifically, will the recipient of the report understand how the controls were selected, evaluated, and scored?



In the case of HITRUST CSF Validated Assessment Reports,[2] the HITRUST CSF®[3] control framework is publicly available and changes are documented extensively in every release. HITRUST's robust assessment approach, control maturity and scoring methodology, and related assurance requirements are also clearly articulated in publicly available guidance.[4, 5, 6]

However, other options may not offer the same clarity. For example, while an AICPA SOC 2 report may specify the controls used to evaluate each of the Trust Services Criteria (TSC) within the scope of the report, information on the controls and how they were selected are only made available to recipients of the report rather than the public at large. Additionally, while the approach used to evaluate the controls follows AICPA guidelines, the specific methods used can vary from one CPA firm to another.

Scalability – Is the assessment approach scalable to any size organization or, more specifically, can any size and type of organization leverage the approach? And does scaling of the control framework follow formal guidelines for tailoring the controls to the organization?



The HITRUST CSF leverages a framework-based risk analysis[7] to integrate and harmonize requirements from more than 40 relevant standards, best practice frameworks, and regulations, which allows organizations to scale their control requirements based on specific risk factors and ensure they appropriately manage information risk and compliance. They can also select from a variety of assessment options (e.g., Rapid, Readiness, and Validated Assessments) based on the inherent risk of their operations. This makes the HITRUST CSF suitable for organizations of all types and sizes, regardless of industry. HITRUST's Authorized External Assessor Program[8]—supported by a pool of approximately one hundred independent HITRUST Authorized External Assessor Organizations ranging from large global professional services firms to small boutique consultancies—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.

While NIST, for example, provides a comprehensive control framework that is also tailorable[9]—albeit not as straightforward as the HITRUST CSF—NIST does not provide, manage, or otherwise support a controls assessment and reporting program for use in the private sector.

Consistency – Are assessment results consistent regardless of the professional or professional services firm engaged? Or more specifically, does the process ensure that individuals performing the work are evaluating and documenting their findings consistently? Does the assessment approach minimize variance and inconsistencies?

In the case of HITRUST, professional services firms and consultancies participating in the HITRUST Authorized External Assessor Program[10] are vetted by HITRUST and required to utilize professionals who are trained and certified[11] in the application of HITRUST's prescriptive assessment and assurance methodologies on every engagement. The results of all HITRUST CSF Validated Assessments are also captured along with supporting evidence and are scored and reviewed automatically using a single assessment platform. This helps ensure assessments are consistent, whether they are different assessments performed by the same individuals or similar assessments performed by different individuals. And, due to the resulting high level of consistency, HITRUST can provide organizations with valuable information risk and compliance benchmarks with every HITRUST CSF Validated Assessment.

On the other hand, NIST—while it does provide extensive control assessment guidance—neither trains nor vets assessors that perform NIST-based control assessments in the private sector.

Accuracy – Do assessment results accurately reflect the state of controls implemented in an organization's environment? Or more specifically, what mechanisms are in place to facilitate the accurate evaluation and scoring of implemented controls?

HITRUST provides the only assessment report that clearly articulates control maturity using its innovative PRISMA-based, quasi-quantitative control maturity and scoring model[4], lending a degree of accuracy simply not achievable by traditional assessment approaches, i.e., yes/no.

None of the other major controls assessment and reporting options utilize such an approach, and some assessment options like NIST may rely on self-attestation, which are often inaccurate[12] when used in the private sector.

Integrity - Are assessments conducted and the results reported consistent with prescribed requirements for the assessment and reporting option? Or more specifically, what processes are in place to ensure the assessor conducted the assessment faithfully and reported the results truthfully?

Governed by a Quality Assurance Subcommittee of its Board of Directors, overseen and audited by a Compliance department, and managed by an Assurance department, the HITRUST CSF Assurance Program provides a granular level of oversight through a quality control process that reviews each assessment and resulting report it produces. Today, each assessment submitted by an External Assessor undergoes over four dozen automated quality checks to identify and address assessment errors and omissions; in addition, each assessment is handed off to Quality Assurance Analysts within HITRUST's Assurance team for review. The work of the Assurance team is continuously audited by the Compliance team, and quality metrics are reported quarterly to the Board's Quality Assurance Subcommittee, bi-weekly to the HITRUST CEO, and weekly to the Assurance team's leadership.

Any problems with assessments introduced by assessors are quickly identified, corrective actions taken. And—if necessary—systemic quality issues may result in penalties up to and including re-performance of the assessment and/or termination from the HITRUST Authorized External Assessor Program.

Other reporting options also provide some level of vetting and oversight of their respective assessors. For example, AICPA provides audit standards for CPA firms and supports limited peer review of the attestation work performed by a CPA firm, including its internal quality assurance processes. However, no reporting option other than HITRUST provides centralized management and oversight of ***each and every assessment performed*** by its assessors.

Efficiency – Do assessments and their associated reports satisfy multiple stakeholders for multiple purposes? Or more specifically, can the report be used by multiple relying parties?

Since HITRUST has harmonized various relevant information risk and compliance frameworks, best practices, and regulations into a single set of rationalized control requirements, organizations do not need to answer more questionnaires or conduct more assessments than absolutely necessary. And because HITRUST also supports transparency, scalability, consistency, accuracy, and integrity in its assessment and reporting process, it is able to deliver a single, comprehensive assessment report that can provide appropriate assurances for multiple requesting parties via detailed, source-specific scorecards, saving organizations significant time and money—an approach HITRUST calls *Assess Once, Report Many*™.

While ISO 27001 and NIST 800-53, for example, can and have been mapped to many other frameworks and even some regulations, neither control framework actually integrates and harmonizes their requirements. Subsequently, while assessments

against these frameworks can be used to report to multiple entities with similar assurance requirements, a significant amount of work may be required to demonstrate how these assessments support requests for assurance against multiple other standards, frameworks, and regulations.

How do some of the most popular approaches compare when it comes to their overall 'rely-ability'?

Organizations have many options when it comes to assessing and reporting upon their information security and privacy posture; however, not all provide the same level of 'rely-ability', as shown in the table below for some of the most widely used assessment and reporting frameworks: AICPA, HITRUST, ISO, and NIST.

Criterion	Assessment Reporting Option Attribute	AICPA SOC2	HITRUST CSF	ISO 27001	NIST 800-53
Transparency	Open Controls Framework	N/A[13]	Yes	Yes	Yes
	Open Assessment Methodology	Yes[14]	Yes	No	Yes
Scalability	Tailorable Controls Framework	N/A	Yes	Yes[15]	Yes[16]
	Market-based Assurance Program	Yes	Yes	Yes	No
Consistency	Prescriptive Control Assessment Methodology	Yes[17]	Yes	No	Yes
	Trained, Vetted Assessor Pool	Yes[18]	Yes	Yes[19, 20]	No
Accuracy	Maturity-based Implementation Model	No	Yes	No	No
	Quasi-quantitative Scoring Approach	No	Yes	No	No
Integrity	Formal Assessor Program	Yes[21]	Yes	Yes	No
	Centralized Quality Assurance	No	Yes	No	No
Efficiency	Integrated & Harmonized Control Framework	N/A[22]	Yes	No	No
	Standardized Report w/ Optional Scorecards	Yes[23]	Yes	No	No

While other assessment and reporting options may provide an open control framework, many lack transparency in how the controls are derived, updated, or assessed. These frameworks are often "one size fits all" and not easily scalable to different types and sizes of organizations; and most of the available options do not leverage a control maturity model or quasi-quantitative scoring approach, which impacts the accuracy of the results. There are no other options that provide a vetted and trained independent assessor pool, the lack of which can result in inconsistent assessment and reporting; and, while some may provide some type of training and vetting of assessors, none of the other options provide centralized quality assurance of assessment and reporting, the lack of which can adversely impact overall integrity of the assurances provided. And most of the other available options are single purpose, resulting in less efficiency when reporting to multiple stakeholders.

So which assessment and reporting option provides the most 'rely-able' assurances?

HITRUST has spent the last 12 years architecting and implementing a comprehensive and fully integrated approach to information risk management and compliance assessment and reporting that provides a level of transparency, scalability, consistency, accuracy, integrity, and efficiency simply not obtainable through other approaches. HITRUST's unique and comprehensive approach to information risk management and compliance—*The HITRUST Approach*—addresses all of these criteria to provide the most robust assurance option available.

For more information visit https://hitrustalliance.net/the-hitrust-approach/

Endnotes

[1] For example, see Cybercrime Magazine (2019). *2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics*. Available from https://cybersecurityventures.com/cybersecurity-almanac-2019/.

[2] Cline, B. and Huval, J. (2019). *Leveraging HITRUST CSF Assessment Reports: A Guide for New Users*. Frisco, TX: HITRUST. Available from https://hitrustalliance.net/content/uploads/Leveraging-CSF-v9-Assessment-Reports.pdf.

[3] HITRUST. (2019). *HITRUST CSF*. Available from https://hitrustalliance.net/hitrust-csf/.

[4] Vander Wal, K., Frederick, M., Cline, B., Huval, J., and Sheth, B. (2019, Mar.). *CSF Assessment Methodology*, Ver. 9.2. Frisco, TX: HITRUST. Available from https://hitrustalliance.net/content/uploads/CSFAssessmentMethodology.pdf.

[5] Cline, B., Huval, J., and Sheth, B. (2018, Feb.). *Evaluating Control Maturity Using the HITRUST Approach: Quasi-quantitative scoring based on the HITRUST CSF security and privacy control implementation maturity model*. Frisco, TX: HITRUST. Available from https://hitrustalliance.net/content/uploads/Evaluating-Control-Maturity-Using-the-HITRUST-Approach.pdf.

[6] Vander Wal, K., Frederick M., Huval, J., and Sheth, B. (2019, Oct.). *HITRUST CSF Assurance Program Requirements*, Ver. 9.3. Frisco, TX: HITRUST. Available from https://hitrustalliance.net/content/uploads/CSFAssuranceProgramRequirements.pdf.

[7] Cline, B. (2017, Sep.). Leveraging a Control-Based Framework to Simply the Risk Analysis Process. I*SSA Journal*, 15(9), pp. 39-42. Available from https://hitrustalliance.net/content/uploads/2016/01/Leveraging-a-Control-Based-Framework-to-Simplify-the-Risk-Analysis-Process.pdf.

[8] HITRUST. (2019). *External Assessors*. Available from https://hitrustalliance.net/external-assessors/.

[9] Joint Task Force Transformation Initiative. (2013, Apr.) *Security and Privacy Controls for Federal Information Systems and Organizations* (NIST SP 800-53 Rev 4), Chapter 3. Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[10] Vander Wal, K., Frederick, M., Datel, M. (2019). *HITRUST External Assessor Requirements*. Frisco, TX: HITRUST. Available from https://hitrustalliance.net/content/uploads/ExternalAssessorRequirements.pdf.

[11] HITRUST. (2019). *HITRUST Academy*. Available from https://hitrustalliance.net/hitrust-academy/.

[12] Cline, B. (2019). (2019, Nov 11). *Understanding and Improving the Role of Self-assessments in Third-party Risk Management*. Featured on HITRUST [Blog post]. Available from https://blog.hitrustalliance.net/understanding-improving-role-self-assessments-third-party-risk-management/2/.

[13] SOC 2 is a reporting framework rather than a control framework; it does not provide the controls needed to achieve the outcomes specified by the AICPA TSC.

[14] AICPA (2018, Jan 1). *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*. Chicago: Author. Available from https://www.aicpastore.com/*/AuditAttest/IndustryspecificGuidance/PRDOVR~PC-0128210/PC-0128210.jsp.

[15] ISO provides additional guidance around implementing its controls in various other 27XXX documentation.

[16] Joint Task Force Transformation Initiative. (2013, Apr.).

[17] AICPA (2018, Jan 1). *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*. Chicago: Author.

[18] AICPA SOC 2 engagements are performed by CPAs via CPA firms.

[19] ISO. (2019). *Certification & Conformity: Conformity Assessment*. Available from https://www.iso.org/conformity-assessment.html. ISO does not perform conformity assessments or provide certification.

[20] ANSI. (2019). ANSI National Accreditation Board. Available from https://anab.ansi.org/management-systems. ANSI accredits certification bodies that can certify management systems such as ISO 27001.

[21] SOC 2 reports must be signed by a CPA and follow AICPA standards.

[22] SOC 2 is a reporting framework, and AICPA does not specify the controls needed to address the objective-level Trust Services Criteria used in the report.

[23] Although SOC 2 reports do not inherently address a control framework other than the one used, if any, to provide the controls needed to address the TSC used in the report, this information regarding their relationship to other frameworks could be included in a section titled 'unaudited information' in an appendix.