HITRUST®

The Assurance Intelligence Engine™

How HITRUST Uses Automated Verification and Validation to Improve Rely-ability

February 2022

Table of Contents

Introduction

Threats to personal data[i] have increased significantly over the past decade resulting in a similar increase in the number and severity of data breaches in both the public and private sectors. The inability of many organizations to react to this changing threat environment has subsequently resulted in a similar increase in regional (state), national, and international regulatory oversight, which has firmly established a duty of care[ii] for the protection of personal data and individual privacy.[iii] The need for organizations to demonstrate an appropriate standard of care[iv] for personal data—or receive similar demonstrations from relevant third parties—is simply no longer up for debate.

Unfortunately, organizations are inundated with a wide array of best practice and risk management frameworks and assessment approaches with varying levels of rigor and independence. These typically include assessments of risk based on proprietary questionnaires—often self-attested or assessed—or, more recently, 'reputation scorecards' based on the evaluation of publicly accessible information—as well as traditional audits, inspections, and assessments conducted by an independent party. It can be difficult for organizations to determine a suitable assurance strategy, especially for those that seek a level of assurance commensurate with the risks incurred by a third-party relationship.

Assurance

Although HITRUST®[v] Assessments are also used by organizations to help substantiate the controls they specify,[vi] their primary function is to provide what the National Institute of Standards and Technology (NIST) refers to as a current profile for cybersecurity based on a controls gap assessment of its target profile.[vii] The assessment is used to provide a level of assurance around its current profile via a formal report intended for consumption by relevant stakeholders such as internal leadership, business partners, customers, and regulators (also referred to as 'relying parties').

To better understand how different assessment/audit and reporting approaches result in different levels of assurance—whether provided through HITRUST®[viii] or by, or on behalf of, another standards development organization (SDO)—we need to agree on what the term means.

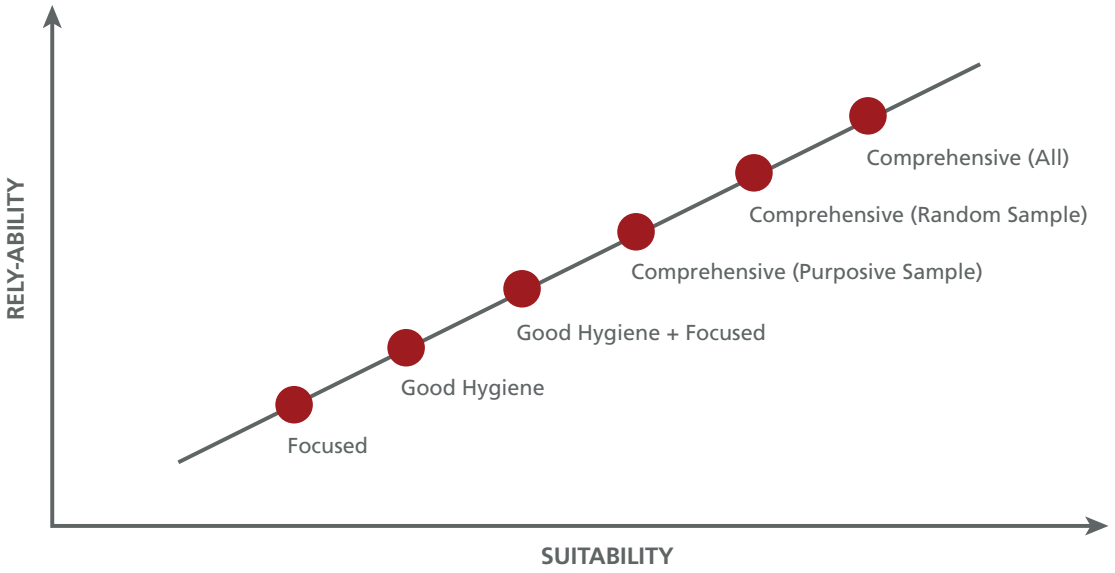
NIST defines assurance in several ways, two of which are as: (1) "a measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy [and (2)] the grounds for confidence that the set of intended security controls in an information system are effective in their application." Integral to these definitions is the idea of confidence or trustworthiness, which may be defined as "worthy of confidence" or more specifically, "being or deriving from a source worthy of belief or consideration for evidentiary purposes." It is this level of confidence or trustworthiness that allows an entity to rely upon the information provided by an assessment/audit and how it is reported.

By parsing the NIST definitions in this way, we subsequently propose three principal aspects or 'dimensions' of assurance.

Suitability is intended to address the 'security features, practices, procedures, and architecture'—i.e., the information security protections or 'controls' for an appropriate scope of assessment—that are the subject of the intended assurances. We can further stipulate that the controls must be reasonable and appropriate for the organization and must provide for the adequate protection of sensitive information within the context of assessment, e.g., the controls must manage risk to a level deemed acceptable by the organization.

Figure 1 provides a depiction of the relative suitability of an assurance approach based on the comprehensiveness of the controls being assessed.

Figure 1. Relative Suitability



Our first use of *Focused* refers to an assessment/audit of a set of controls related to a specific area of interest or concern, e.g., access controls in general or something more specific like recertification of user access rights. While the controls may be 'suitable' for the intended purpose, such a focused assessment/audit does not convey significant information about the state of an organization's overall information protection program and would likely not find much additional utility save perhaps its use as evidence in another assessment.

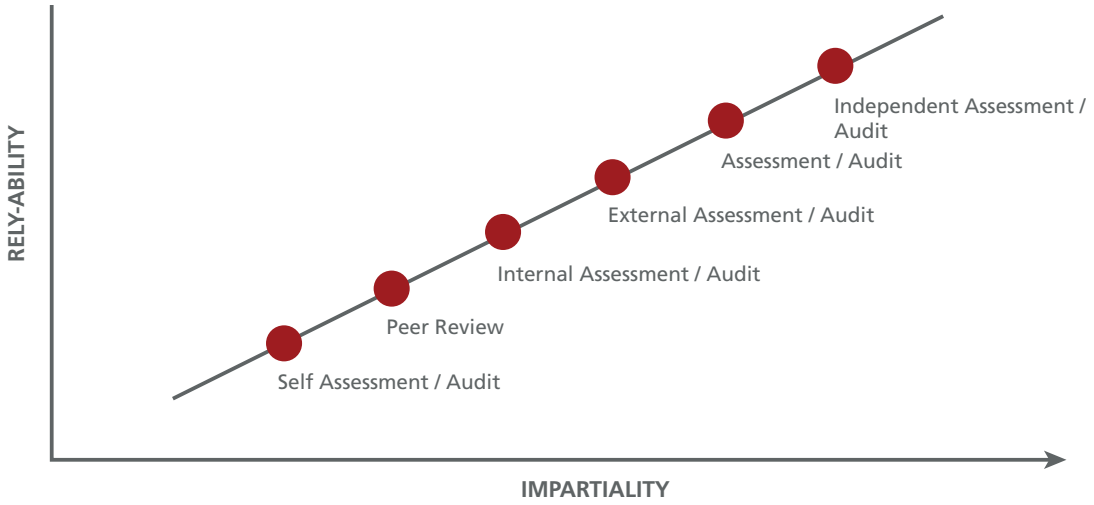
Good Hygiene refers to a broader set of controls that are considered to be minimal best practice for almost any organization, whereas *Good Hygiene + Focused* refers to an assessment/audit that includes good hygiene security requirements but is also augmented with additional control requirements relevant to what is being assessed or audited, e.g., an assessment/audit intended to address general regulatory requirements such as the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (HSR) for electronic protected health information (ePHI) or perhaps something more specific such as the Payment Card Industry (PCI) Data Security Standard (DSS) for cardholder information.

The last three types of assessment/audit all include a comprehensive 'population' of controls typically specified as the result of a similarly comprehensive risk analysis of all reasonably anticipated threats to the organization's sensitive information. However, *Comprehensive (Purpose Sample)* refers to an assessment/audit of a subset (sample) of a comprehensive set of controls (population) that is determined based on a specific rationale, referred to as a 'purposive sample of a typical instance.' HITRUST Certification[ix] is based on such an approach, as the intent is to provide reasonable assurances about the state of an organization's information protection program at a reasonable cost. *Comprehensive (Random Sample)* simply refers to a subset (sample) of a comprehensive set of controls (population) that are selected randomly. Last, *Comprehensive (All)* refers to an assessment/audit of the entire set of controls that are applicable to a specific scope of assessment or audit, e.g., a HITRUST Validated Assessment that includes all the controls in the framework—commonly referred to as a 'comprehensive assessment'—or those assessments typically performed by U.S. government agencies as required under the Federal Information Security Management Act (FISMA).

Impartiality is intended to address the 'measure' or 'grounds for confidence' needed by a relying party in an assessment—whether the assessment/audit is 'worthy of belief or consideration for evidentiary purposes'—via the amount or level of independence between the assessor/auditor and the entity being assessed or audited. The level of impartiality can also be supported by an objective quality assurance review and automated quality checks that address consistency of responses and supporting evidence.

Figure 2 is intended to depict the relative impartiality of an assurance approach based on the relationship of the assessor/auditor to the organization or business unit that is the subject of assessment or audit.

Figure 2. Relative Impartiality



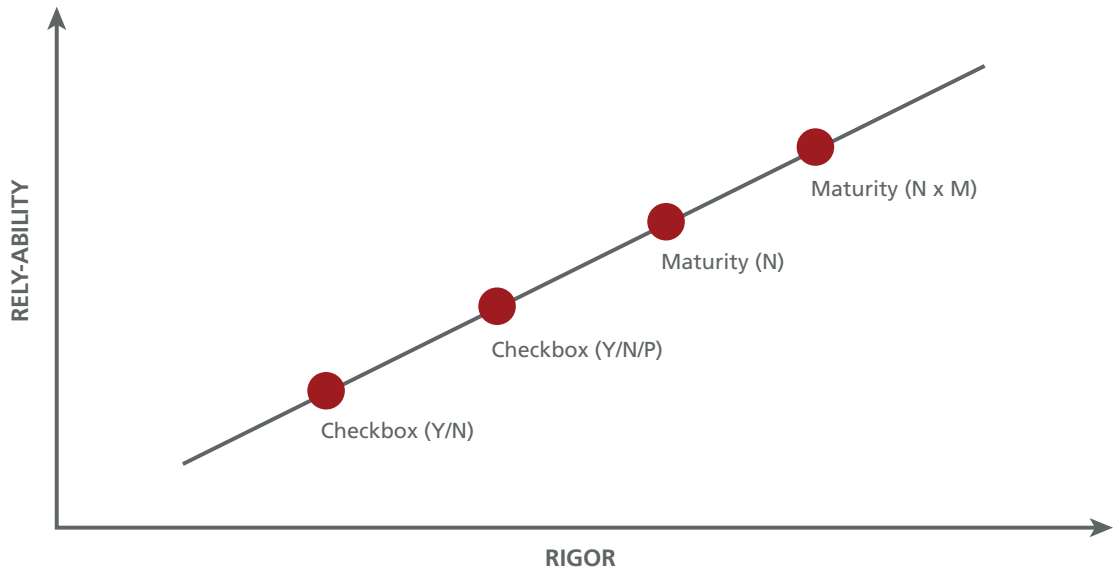
Self-Assessment/Audit refers to assessment or audit conducted by an entity upon itself. *Peer Review* is similar, but controls are evaluated by one or more individuals other than the control owner with similar competencies but generally don't have the same level of independence as an internal assessment or audit function (e.g., a review of perimeter security controls conducted by an assurance function that reports to the CISO). *Internal Assessment/Audit* refers to an independent function within the organization that conducts assessments or audits on other parts of the organization, whereas *External Assessment/Audit* refers to a professional service offered by an independent third party but for which the actual assessment/audit[x] service is paid for by the subject of the assessment or audit. We use *Independent Assessment/Audit* here to refer to an assessment or audit that is conducted by an independent third party but for which the assessment/audit service is paid by an entity other than the subject of the assessment or audit, e.g., a business partner, customer, or regulator.

Rigor

Rigor provides the "grounds for confidence that the set of intended security controls in an information system are effective in their application," which is generally based on the accuracy and precision supported by the assurance approach. Rigor is impacted by evaluation and scoring models, advanced quality reviews based on relationships between and amongst the methodologies, assessment guidance, assessor/auditor qualifications and training, and other factors.

Figure 3 illustrates the relative rigor of an assurance approach based on the evaluation and scoring model employed.

Figure 3. Relative Rigor

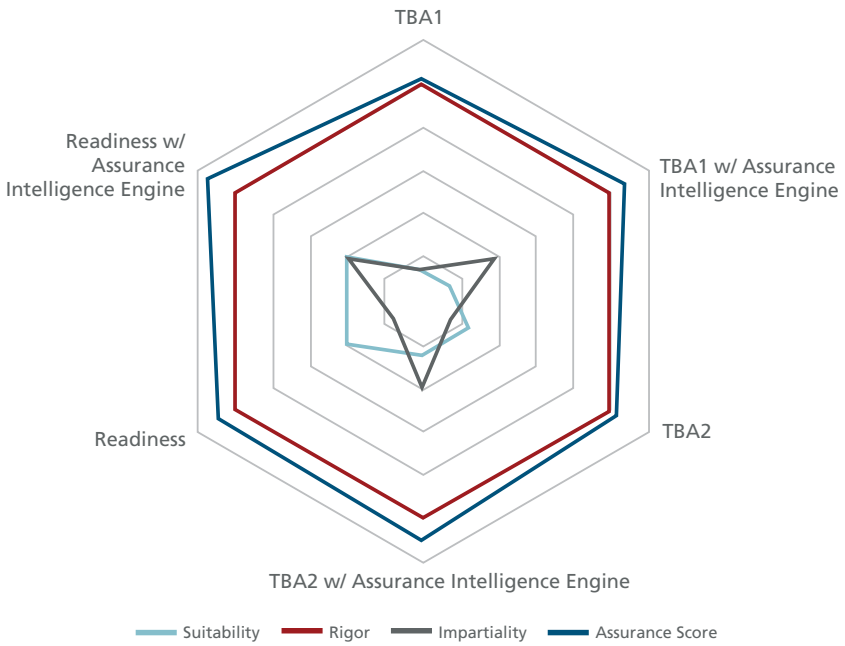


Checkbox (Y/N) refers to a 'traditional' approach to evaluating controls that simply determines whether or not a control is in place. Fortunately, this type of assessment/audit approach is not used as much as it once was. Instead, we see a more rigorous *Checkbox (Y/N/P)* approach that identifies when controls may be implemented (Y), not implemented (N), or only partially implemented (P,) and typically offers recommendations for improvement. *Maturity (N)* models expand on the *Checkbox (Y/N/P)* approach by evaluating a control's capability based on the achievement of N, increasingly rigorous levels of maturity. For example, the Systems Security Engineering Capability Maturity Model (SSE-CMM) evaluates five levels of process maturity: Performed Informally, Planned and Tracked, Well Defined, Quantitatively Controlled, and Continuously Improving.[xi] The maturity assigned to a control would be the highest level that is fully achieved. Another example is the maturity model employed by NIST's Program Review for Information Security Management Assistance (PRISMA) assurance approach that similarly uses five levels of maturity but which are more suited to security control assessments/audits: Policies, Procedures, Implementation, Testing, and Integration. And finally, *Maturity (N x M)* expands on the Maturity (N) model by evaluating *M* degrees of compliance with the requirements for each of the *N* maturity levels. The only known example of such an approach is the HITRUST CSF control maturity and scoring model, which is based on the PRISMA model but evaluates five levels of compliance for each of the five levels of control maturity in the model: Policy, Procedure, Implemented, Measured, and Managed.[xii] The HITRUST CSF control maturity and scoring model also allows organizations to use the results from a HITRUST Assessment to estimate the relative likelihood of a control failure.

Objective Rating of Assurance Approaches

Further, by evaluating an assurance approach along the three dimensions of assurance based on a standard set of relevant characteristics, it is possible to provide an objective rating of the approach's overall rely-ability.[xiii] An example using a simple vector-based rely-ability rating model for current HITRUST assessment types leveraging the information provided previously is provided by Figure 4 on the following page.

Figure 4. Relative Rely-ability of HITRUST Assessments



The HITRUST *Rapid* Assessment is a self-assessment of good-hygiene controls using a Maturity (N x M) approach. *TBA1* and *TBA2* are two HITRUST assessments that are currently in development and subsequently yet to be announced (TBA): *TBA1* is a self-assessment of good-hygiene controls using a Maturity (N x M) evaluation model, and *TBA2* is a self-assessment of good hygiene plus additional focused controls that also uses a Maturity (N x M) model. The HITRUST *Readiness* Assessment is a self-assessed[xiv] version of the HITRUST *Validated* Assessment based on a purposive sample of a comprehensive set of controls using a Maturity (N x M) model for their evaluation.

HITRUST is currently working on a more precise rely-ability scoring model that examines multiple quality indicators of an assessment approach for each of the three dimensions of assurance, the details of which will be released in a future paper.

Improving Rely-ability

Threats to Rely-able Assurance

In general, an 'assurance assessment' can be performed by the subject of the assessment (self-assessment/audit) or by someone else (external or independent audit/assessment). Both types of assessment have their advantages and disadvantages; however, it can safely be said that—with all else being equal—a self-assessment/audit will always be less rely-able than an external or independent audit/assessment.

Self-assessments/audits are generally subject to more error than their external or independent counterparts due to a lack of expertise, self-bias, or even potential malfeasance. Many organizations, especially smaller ones, typically lack the expertise needed to conduct an assessment or audit of their security features, practices, procedures, and architecture correctly. Experience has also shown that an organization with a very immature information protection program will tend to rate itself during a self-assessment/audit much higher than the underlying evidence would otherwise suggest, whereas an organization with more robust programs tends to be 'closer to the mark' when compared with an external or independent audit or assessment. We have also seen organizations intentionally boost their self-assessment results to maintain or obtain a specific business relationship.

This is why HITRUST generally recommends limiting the use of self-assessments to (1) vetting smaller entities that present inherently low risk to an organization or (2) 'readiness' assessments in advance of a future independent assessment, if needed. Both use cases have been part of the HITRUST Approach[xv] for almost a decade.

While generally more rely-able, external/independent audits and assessments can also be subject to error for a variety of reasons, including: gaps in auditor or assessor knowledge and expertise going into the audit or assessment; the type and rigor of the audit or assessment, analytical procedures, and review during the audit or assessment process; the quality and accuracy of the reports coming out of the audit or assessment; and potential issues related to the context of the audit or assessment such as "abnormal audit [or assessment] fees, audit [or assessment] tenure, audit [or assessment] partner compensation, and audit [or assessment] fee premiums, all of which may influence auditor incentives."[xvi]

The Role of Quality Assurance

To help address many of these issues, all HITRUST Validated Assessments are conducted by trained and vetted HITRUST Authorized External Assessors, based on a robust control maturity and scoring model, supported by a standard assessment and reporting model, and reviewed by a dedicated team of quality assurance (QA) analysts to help ensure the highest level of rely-able assurance.

The purpose of QA is to help ensure something's relevance,[xvii] e.g., that the end result of a process meets or exceeds stakeholder expectations. As applied in the context of the HITRUST Assurance Program™,[xviii] the role of quality assurance is to ensure the relevance—i.e., the overall 'rely-ability'—of a HITRUST Validated Assessment Report.

HITRUST has been performing manual QA reviews of all HITRUST Validated Assessments since the HITRUST CSF and Assurance Program were first introduced in 2009. However, although the end result is a more rely-able HITRUST Validated Assessment Report than what would have otherwise been possible without such a review, manual QA reviews consume an extensive amount of time and resources to conduct. To aid in the automation of the QA process and improve process efficiency, as well as the overall rely-ability of the assurances provided by the HITRUST Approach, HITRUST subsequently looked to the field of information systems security engineering (ISSE) and the distinction it makes between verification and validation testing conducted during the system development life cycle (SDLC).

Verification is a process used to help ensure a system meets specifications, i.e., that it is built correctly.[xix] Verification can be incorporated into the assessment quality assurance review process through the use of checks to verify the *completeness* of assessment documentation, the *consistency* of data points present in assessment documentation, and the *correctness* of an assessment's conclusions. An example of a completeness-focused verification check is determining whether documented rationales exist for all requirements designated as not applicable to the scope of the assessment. An example of a correctness-focused verification check is determining whether the provided physical addresses of all facilities included in the scope of the assessment exist in the U.S. Postal Service database. An example of a consistency-focused verification check is determining whether the systems included in the scope of the assessment are the same everywhere they are enumerated in the assessment documentation.

On the other hand, ***Validation*** is a process used to help ensure the system meets stakeholder expectations, i.e., that the correct system is being built.[xx] Validation is also important as it helps determine whether the subject of validation "is trustworthy and suitably represents reality."[xxi] Validation can also be incorporated into assessment quality assurance reviews through the use of checks to help ensure the *completeness* of assessment documentation, the *consistency* of data present in assessment documentation, and the *correctness* of assessment conclusions. An example of a consistency-focused validation check is determining whether a particular technology (e.g., wireless networks) is uniformly described as either 'in' or 'out' of the assessment scope. As another example, a correctness-focused validation check might examine whether a documented policy actually addresses the specific control requirements to which it is linked. A simple version of this check would determine

whether the policy name or description includes one or more keywords related to the requirement (e.g., encryption, access, or privacy). A more complex validation check, arguably one that would leverage machine learning or artificial intelligence to implement, would be scanning the content of a documented policy for language that is semantically similar to the linked control requirement. A sophisticated validation check like this could also determine how completely the requirement was addressed and potentially obviate the need for manual review by an analyst.

Given that verification and validation both address elements of *completeness*, *correctness*, and *consistency*, it can be difficult at times to distinguish them apart. The key is to determine whether a particular check is meant to evaluate how well the assessor put the assessment documentation together (verification) or if the check is meant to evaluate the general accuracy or truthfulness of the information in the assessment documentation and ultimately the reliability of the assurances provided (validation). To address this issue, checks that inadvertently address both verification and validation are generally parsed into two separate checks that maintain separation between the two, as a verification component of a conflated check should not inadvertently flag a manual review nor should it be considered in an evaluation around the accuracy or truthfulness of the information provided.

The Assurance Intelligence Engine

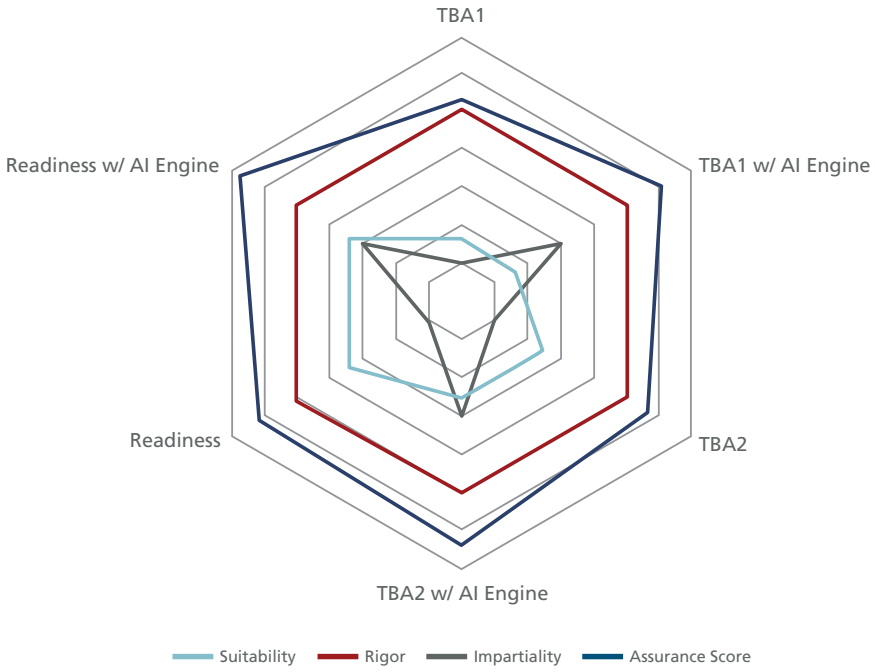
HITRUST began using a combination of real-time and retrospective automated verification and validation checks to support its QA review of HITRUST Validated Assessments in early 2019. The result has been an improvement in the quality of HITRUST Validated Assessments submitted by External Assessors as well as shorter processing times for the review and subsequent issuance of HITRUST Validated Assessment Reports. The use of automated verification and validation and the supporting technologies that HITRUST continues to innovate to perform these functions are collectively referred to as the Assurance Intelligence Engine.

The Assurance Intelligence Engine uses a new patent-pending approach designed and developed by leveraging HITRUST's more than 13 years of compliance assessment experience, best-in-class quality assurance methodologies, and data analytics on hundreds of thousands of assessments submitted by organizations of varying sizes, industries, complexities, and locales. Use of the AI Engine improves the overall rely-ability of assessment deliverables by analyzing assessment documentation for oversights, inconsistencies, and errors. The AI Engine adds efficiency to HITRUST's comprehensive QA reviews by adding a layer of automated checks which complement existing, manual QA review procedures. Fully incorporated into the HITRUST MyCSF®[xxii] SaaS information risk management and assessment platform in Q1 2021, the Assurance Intelligence Engine measurably increases assurances delivered through HITRUST Assessments.

The AI Engine also helps to detect potential issues in real-time while assessments are underway. During the assessment process, the AI Engine proactively identifies potential issues by performing a real-time analysis against thousands of data points across the body of documentation produced during assessments. Through the MyCSF® platform, the AI Engine provides detailed descriptions of identified potential quality issues along with the identification of the triggering data point(s) and recommended remedial actions.

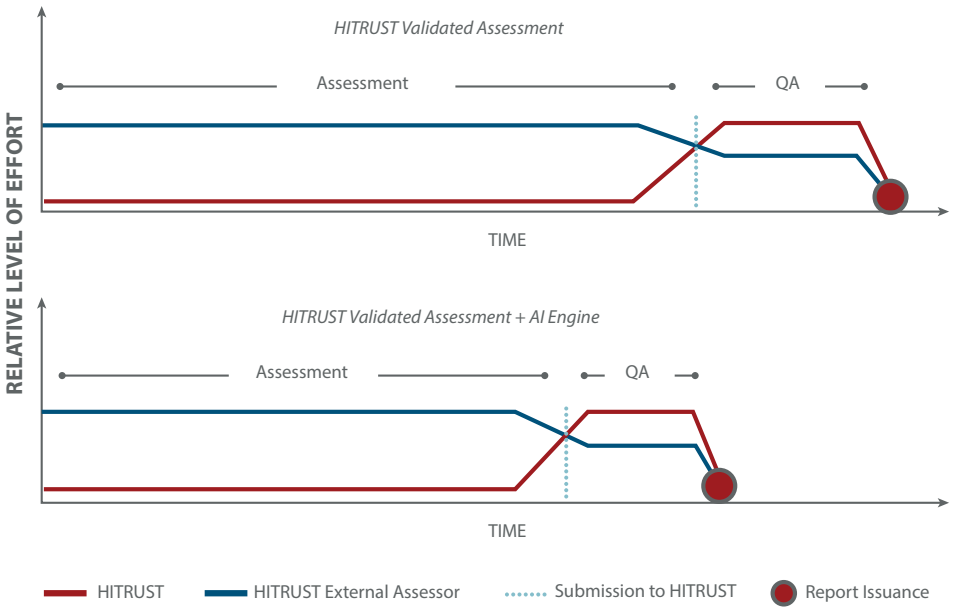
Providing independent, real-time feedback while completing a HITRUST Readiness Assessment allows assessed entities to provide more accurate and complete information about their information protection programs and increases the overall rely-ability of the assurances provided.

Figure 5. Increased Rely-ability of Self Assessments



Feedback provided through the AI Engine also allows both HITRUST Authorized External Assessors and assessed entities to provide more accurate assessment submissions and reduce the time it takes HITRUST's centralized reporting and oversight function to complete the QA process and issue official reports, as seen in the following figure.

Figure 6. Improved Efficiency of Quality Assurance



Additionally, the AI Engine will allow HITRUST to expand its portfolio of assessment offerings in the future to provide organizations with assurance reporting options that can be used to satisfy any business need.

Conclusion

The business of providing assurances that appropriate security controls are in place is complex and ever-changing. The challenges continue to increase as cyber threats evolve, compliance requirements change, and IT environments become increasingly complex. Today more than ever, organizations need to provide assurances related to information risk management and compliance programs to internal and external stakeholders; doing so requires a reliable assurance report produced through a consistent and accurate assurance process.

With the addition of the Assurance Intelligence Engine, HITRUST can increase efficiency and continue to pave the way for providing more rely-able assurances. And given the lengthy and complex documentation produced through any security and privacy assessment, HITRUST believes External Assessors and assessed entities will appreciate having the AI Engine working behind the scenes to identify and alert on potential issues buried their assessment's narratives, supporting artifacts, and metadata.

About HITRUST

HITRUST—a leading privacy and security standards development organization[xxiii] (SDO) in the private sector—has been at the forefront of helping industry define a minimum standard of due diligence[xxiv] and due care[xxv] for the protection of personal data and individual privacy since 2009 with the first release of the HITRUST CSF and implementation of the Assurance Program.

> If you haven't spent the time to educate yourself on the HITRUST Assurance Program and the HITRUST CSF, you may think that it's just another 'check-box'-style controls assessment. This could not be further from the truth. In fact, the framework is much more involved and comprehensive; and after delving into the program, it's easy to see how it's ultimately designed to mature an organization's security posture.
>
> The rigor, the independence factor, the review, the analysis, the validation, and the quality assurance that are built into the HITRUST CSF validation process well exceeds what you may find in other 'open' frameworks.[xxviii]

By incorporating numerous international, federal, and state governmental regulations as well as recognized standards such as ISO 27001[xxvi] and NIST SP 800-53,[xxvii] the HITRUST CSF® helps organizations address information risk management and compliance challenges through a comprehensive, risk-based, flexible framework of prescriptive and scalable controls. And by including both privacy and security standards, the HITRUST CSF uniquely enables organizations to address the big picture of personal data protection. Most privacy regulations require appropriate security measures, which the HITRUST CSF helps organizations identify quickly and easily.

The HITRUST CSF further encourages cooperation between privacy and security functions and assists organizations in achieving better compliance with regulatory requirements and industry-accepted best practices by supporting the conduct of a single, comprehensive assessment of both programs and providing needed assurances to both internal and external stakeholders. Through the HITRUST Assurance Program, organizations who obtain HITRUST Certification covering both privacy and security can readily demonstrate they are achieving reasonable standards of due diligence and due care for their protection.

In fact, HITRUST is the only SDO that provides a comprehensive yet highly tailorable privacy and security control framework that can be applied to any organization in any industry, nationally or globally as well as a robust approach to certification supported by (1) a standardized assessment methodology based on a rigorous control implementation maturity and scoring model, (2) qualified, independent assessor organizations with requisite training and experience in the control framework and assurance approach, and (3) formal oversight and review of every assessment submitted for certification.

Endnotes

[i] **Personal data** is defined here to mean "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (https://gdpr-info.eu/art-4-gdpr/). A natural person may be defined as "a human being as distinguished from a person (as a corporation) created by operation of law" (https://dictionary.findlaw.com/definition/natural-person.html).

[ii] **Duty of care** may be defined as "the legal responsibility of a person or organization to avoid any behaviors or omissions that could reasonably be foreseen to cause harm to others" (https://legaldictionary.net/duty-of-care/) or as "a duty to use due care toward others in order to protect them from unnecessary risk of harm" (https://dictionary.findlaw.com/definition/duty.html). Duty may be defined as "asks, service, or functions that arise from one's position" (https://dictionary.findlaw.com/definition/duty.html). Care may be defined as "watchful or protective attention, caution, concern, prudence, or regard usually towards an action or situation" (https://dictionary.findlaw.com/definition/care.html). Responsibility may be defined as "a particular obligation for which an individual is to be held accountable, in order to remain an upstanding member of a group or community" (https://legaldictionary.net/responsibility/).

[iii] (Individual) **privacy** may be defined as "freedom from unauthorized intrusion; state of being let alone and able to keep certain esp. personal matters to oneself" (https://dictionary.findlaw.com/definition/privacy.html).

[iv] **Standard of care** may be defined as "the degree of care or competence that one is expected to exercise in a particular circumstance or role" (https://www.merriam-webster.com/legal/standard%20of%20care; https://dictionary.findlaw.com/legal-terms/s.html), where standard may be defined in this context as "something established by authority, custom, or general consent as a model, example, or point of reference [… of the reasonable person]" (https://dictionary.findlaw.com/definition/standard.html).

[v] For more information about the **HITRUST CSF**, see https://hitrustalliance.net/product-tool/hitrust-csf/.

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

[vii] For more information on the **NIST Cybersecurity Framework**, see https://www.nist.gov/cyberframework.

[viii] For more information on **HITRUST**, see https://hitrustalliance.net/about-us/.

[ix] For more information on **HITRUST Certification**, see https://hitrustalliance.net/hitrust-csf/.

[x] By **actual assessment/audit services**, we are referring to the actual conduct of the assessment/audit vice any ancillary services such as independent quality assurance review or report generation.

[xi] Ferraiolo, K. (2000, Oct 19). The Systems Security Engineering Capability Maturity Model (SSE-CMM). *In Proceedings of the 23rd National Information Systems Security Conference*, Slide 21. Available from https://csrc.nist.gov/csrc/media/publications/conference-paper/2000/10/19/proceedings-of-the-23rd-nissc-2000/documents/papers/916slide.pdf.

[xii] Cline, B. (2019, Sep). *Risk Analysis Guide for HITRUST Organizations & Assessors: A guide for self and third-party assessors on the application of HITRUST's approach to risk analysis*, HITRUST: Frisco, Tx, pp. 9 – 10. Available from https://hitrustalliance.net/uploads/RiskAnalysisGuide.pdf.

[xiii] **Rely-ability** is a term used by HITRUST as the ability to rely upon, or trust, information provided by another.

[xiv] A HITRUST Readiness Assessment is based on a self-assessment but utilizes the tools and methodologies of the Assurance Program.

[xv] For more information on the **HITRUST Approach**, see https://hitrustalliance.net/the-hitrust-approach/.

[xvi] Knechel, W., Krishnan, G., Pevzner, M., Shefchilk, L., and Velury, U. (2012, Oct). Audit Quality: Insights from the Academic Literature. In *Auditing: A Journal of Practice and Theory*, 32(1), p. 8.

[xvii] **Relevance** may be defined as "having a bearing on or connection with the matter at hand" (American Heritage Dictionary of the English Language, Fifth Edition (2016). Houghton Mifflin Harcourt Publishing Company. Available from https://www.thefreedictionary.com/relevance.

[xviii] For more information on the **HITRUST Assurance Program**, see https://hitrustalliance.net/hitrust-assurance-program/.

[xix] Haskins, C., (Ed.). (2007, Aug). *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*, Version 3.1. INCOSE: San Diego, CA, pp. 4.13, 4.16 – 4.17.

[xx] Ibid., pp. 4.13, 4.16 – 4.17.

[xxi] Ibid., p. L-6.

[xxii] For more information on **MyCSF**, see https://hitrustalliance.net/product-tool/mycsf/.

[xxiii] Sometimes referred to as a standards body, standards developing organization, or standards setting organization, a **Standards Development Organization** (SDO) is an entity that "provides an orderly and systematic formulation, adoption, or application of requirements (standards) used in a particular industry or sector of the economy" (https://definitions.uslegal.com/i/industrial-standards/), or "provides requirements, specifications, guidelines, or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose" (https://www.iso.org/standards.html).

[xxiv] **Due diligence** may be defined as "a reasonable person under the same circumstances would use; use of reasonable but not necessarily exhaustive efforts" (https://dictionary.findlaw.com/definition/due-diligence.html); also called reasonable diligence. **Diligence** may be defined as "earnest and persistent application of effort esp. as required by law" (https://dictionary.findlaw.com/legal-terms/d.html).

[xxv] **Due care** may be defined as "the care that an ordinarily reasonable and prudent person would use under the same or similar circumstances" (https://dictionary.findlaw.com/definition/due-care.html); also called ordinary care or reasonable care.

[xxvi] For more information on **ISO 27001**, see https://www.iso.org/standard/54534.html.

[xxvii] For more information on **NIST SP 800-53**, see https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

[xxviii] Trinckes, J. (2016, May). *HITRUST Certification: Fact or Fiction* (Perspective Paper). Coalfire: Westminster, CO.

HITRUST®

855.HITRUST
(855.448.7878)
www.HITRUSTAlliance.net