January 2024

The HITRUST Approach to i1 Rapid Recertification

How HITRUST leverages acceptance sampling to streamline the recertification process for organizations with a HITRUST i1 Certification

Executive Summary

Since its inception, HITRUST has supported the public and private sectors with the myriad of products, services, and tools that make up the HITRUST Risk Management Framework, or RMF. The RMF's foundation is the HITRUST CSF®, our comprehensive, risk-based information security and privacy control framework that helps organizations address their specific information risk and compliance needs. The HITRUST CSF is further enhanced by our rigorous approach to the specification and assessment of these controls through the HITRUST Assurance™ Program, which helps organizations provide highly 'rely-able' assurances to multiple internal and external stakeholders including executive leadership, shareholders, business partners, and regulators.

The i1 Assessment is designed to address the need for a continuously relevant cyber security assessment that aligns and incorporates best practices and leverages the latest threat intelligence to maintain applicability with information security risks and emerging cyber threats, such as ransomware and phishing. The design and selection of the controls for the i1 Assessment put it in a new class of information security assessment that is "threat-adaptive" – developed to maintain relevance over time as threats evolve and new risks emerge while retiring controls no longer deemed material. The i1 Assessment is intended for organizations needing a moderate level of assurance that delivers transparent, accurate, consistent, and high-integrity results.

Rapid Recertification provides organizations who obtained an i1 Certification (Assessed Entities)[i] even more value through the use of acceptance sampling, a generally accepted approach to evaluating conformance to a standard. The approach allows Assessed Entities and their Authorized HITRUST External Assessor Organizations (External Assessors) to evaluate as little as a third of the requirement statements scored in an original i1 Assessment to maintain their HITRUST i1 Certification. By successfully demonstrating that the control environment has not materially degraded, an Assessed Entity is permitted to roll forward scores from their certified i1 Assessment for the remaining requirement statements – thus using the i1 Rapid Recertification process to reduce the amount of testing required to complete the assessment for an additional year of certification.[1]

The result is a streamlined, cost-effective approach to certifying and recertifying an organization's use of industry-accepted cybersecurity best practices suitable for most organizations when a relying party needs a moderate level of assurance.[2]

1 Requirement statements that required a CAP during the full i1 Assessment are required to be assessed during the i1 Rapid Recertification Assessment.

2 Portions of the Executive Summary and Introduction sections originally appeared on various parts of the HITRUST Website, references for which are included at the end of this paper.

Contents

Table of Contents

List of Figures

List of Tables

Introduction

HITRUST®, since 2007, has been championing and delivering solutions to address the lack of a common understanding around the security and privacy controls needed to safeguard sensitive information and individual privacy. These solutions include:

1. An industry-accepted information security and privacy control framework, the HITRUST CSF®,[ii] that incorporates multiple regulatory requirements and best practice standards and frameworks;
2. A standard, open, and transparent assessment process to provide accurate, consistent, and repeatable assurances around the level of protection provided by an organization; and
3. An industry-recognized certification of an organization's conformity to the protection requirements specified in the HITRUST CSF through the HITRUST Assurance™ Program.[iii]

Together, the HITRUST CSF, HITRUST Assurance Program, and related products, services, tools, and methods make up the HITRUST Risk Management Framework, or RMF.[iv]

The HITRUST i1 Assessment

The HITRUST Implemented, 1-Year (i1) Validated Assessment[v] leverages a proven set of HITRUST-curated controls designed to ensure that an organization is exercising leading security practices to implement a strong and broad cybersecurity program. The i1 Assessment falls between the level of assurance[vi] conveyed by the more foundational HITRUST Essentials, 1-year (e1) Validated Assessment[vii] and the more rigorous HITRUST Risk-based, 2-year (r2) Validated Assessment[viii] with expanded practices.[ix]

HITRUST i1 Rapid Recertification Assessment

After the initial 1-year i1 Certification, a HITRUST i1 Rapid Recertification Assessment dramatically simplifies the i1 recertification process by allowing Assessed Entities[x] and their External Assessors to evaluate a subset of applicable i1 requirement statements to demonstrate that the control environment has not materially degraded since a prior (full) i1 Assessment was performed to obtain certification.

Upon successfully demonstrating that the control environment has not materially degraded, the Assessed Entity is permitted to roll forward scores from their previous, certified i1 Assessment for the remaining requirement statements – thus reducing the amount of testing required to complete the assessment. The i1 Rapid Recertification results in the same i1 Assessment Reports and i1 Certification as a full i1 Assessment.[xi]

Key similarities between the i1 Assessment and the i1 Rapid Recertification Assessment[xii]

The i1 Rapid Recertification Assessment is comparable to the full i1 Assessment in many ways, the most notable of which include:

- Both provide a means to convey information protection assurances over the assessed entity's scoped and implemented control environment through a shareable, final report with certification issued by HITRUST.
- Both use the same i1 requirements resident in the HITRUST CSF and use MyCSF.[xiii]
- Both require an External Assessor to inspect documented evidence to validate control implementation.
- Both require QA through the HITRUST Assurance Program.
- Both leverage the HITRUST Control Maturity Scoring Rubric.[xiv]
- Final results from i1 Rapid Recertification Assessments can be shared through the HITRUST Assessment XChange[xv] and the HITRUST Results Distribution System.[xvi]

HITRUST Approach to i1 Rapid Recertification

HITRUST leverages the concept of acceptance sampling, a statistical approach widely used in the world of quality control, to determine whether the results of a HITRUST i1 Rapid Recertification Assessment may be used to qualify an organization for recertification or if a full HITRUST i1 Assessment must be performed.

Acceptance Sampling

Originally developed by Harold F. Dodge and Harry G. Romig from Bell Labs,[xvii] acceptance sampling is a statistical technique used to estimate the quality of a batch of products or services by testing a random sample of a specific batch or lot[3] of those products or services—*especially when testing is destructive, costly, or time-consuming*—to help decide whether to accept or reject it. It is essentially a compromise between no inspection and 100% inspection.[xviii]

A lot acceptance sampling plan (LASP) provides the approach used to define, evaluate, and count the number of defective or nonconforming[4] items in a lot in which a sample of size *n* will be accepted when there are *c* or fewer nonconformities found or rejected if more than *c* are found. LASPs may be categorized as:

- **Single**, where a single sample is taken and a determination is made based on the number of nonconformities in the sample;
- **Double**, where a second sample may be taken and the results combined with the first sample if the results from the first sample is inconclusive;
- **Multiple**, where more than two samples may be needed to reach a conclusion;
- **Sequential**, where the number of samples is equivalent to the number of items in the lot; and
- **Skip lot**, where only a fraction of the submitted lots is inspected.[xix]

In general, when developing an acceptance sampling plan, regardless of the type used, there are a number of parameters that must be taken into consideration. These parameters include but are not necessarily limited to:

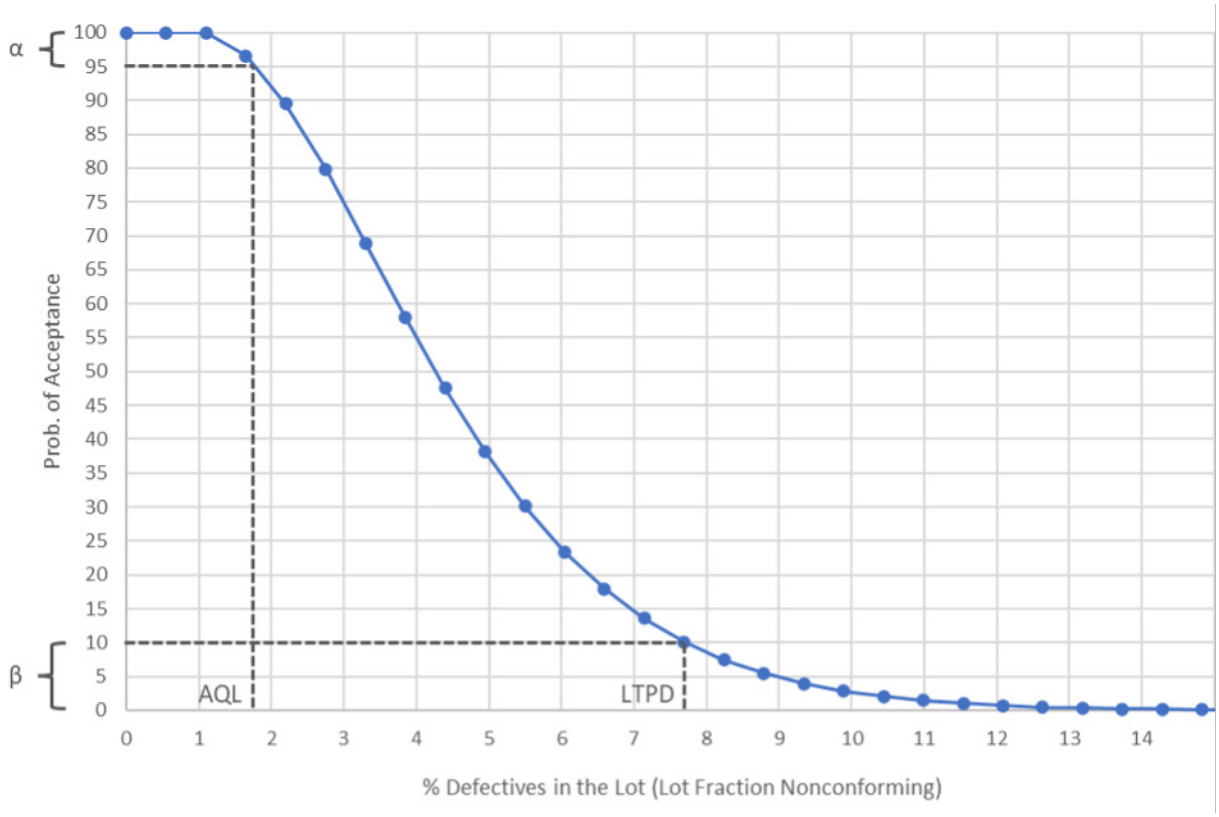
- **Acceptable Quality Limit** (or Level), AQL, which is a percentage of nonconformities that defines a minimum level of quality for the product or service;
- **Lot Tolerance Percent Defective**, LTPD, which is a percentage of nonconformities that would be unacceptable to a consumer;
- **Producer risk** or Type I Error, α, which is the probability of rejecting a lot with an otherwise acceptable quality level (number of nonconformities); and
- **Consumer risk** or Type II Error, β, which is the probability of accepting a lot with an otherwise unacceptable quality level (number of nonconformities).[xx]

The principal tool used in acceptance sampling is the operating characteristic (OC) curve, shown in the following figure, which is a plot of the probability of accepting a lot against the percent or fraction of nonconformities in a lot.

3 We will simply use the term 'lot' going forward.

4 Although synonymous for our purposes, we generally use the terms 'nonconformity' or 'nonconforming' rather than 'defect' or 'defective' going forward (with the exception of Table 1).

Figure 1. OC Curve – Example



HITRUST Implementation

HITRUST views each i1 assessment as a 'batch' of assessed controls for a specific Assessed Entity, which is produced by a defined assessment process—specifically the HITRUST Assessment process[xxi]—that is itself subject to a quality control process. Assuming the HITRUST Assessment and related quality assurance processes are both stable[5] [xxii] and capable,[6] [xxiii] one may also assume the results of a longitudinal series of i1 assessments would either stay the same or improve over time if an organization is to maintain its certification status. We subsequently define a nonconformity as an i1 control requirement that scores less than the score in the original i1 Assessment used for certification due to a material degradation (and not an assessor or other nonmaterial error made in the original assessment).

We chose to use a double sampling plan as, despite their simplicity, a single sampling plan is generally not the most efficient in terms of the average number of samples needed for a specific value of producer risk (or Type I Error). While multiple (sequential) sampling plans could improve this average, we believe the process would be more complicated than needed for our specific purpose and skip lot sampling plans are simply not suitable because a determination must be made for every instance of recertification.[7] We also use the hypergeometric probability distribution to model the probabilities in our OC curve as it "avoids the unnecessary use of approximations such as [those provided by] the binomial or Poisson distributions."[xxiv]

5 A process is stable if special causes of variation have been removed and only common (natural) variation remains.

6 A process is capable if the output from the process is within specified tolerances.

7 In other words, an Assessed Entity cannot be recertified without some level of testing.

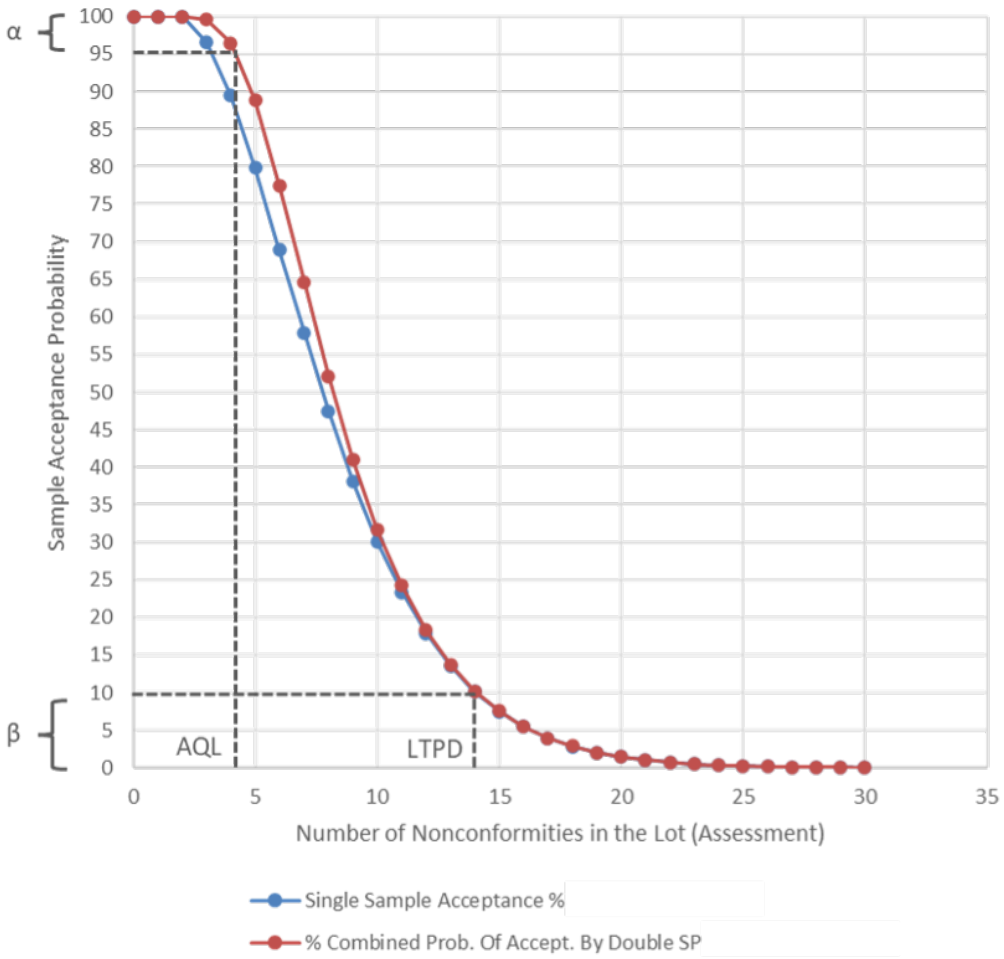
If we select *n* items at random from a population of *N* items without replacement and m items are nonconforming while *N* − *m* items are conforming, then the probability mass function takes the form of the hypergeometric distribution:

$$P(X = x) = f(x) = \binom{m}{x}\binom{N-m}{n-x}\Big/\binom{N}{n}$$

where the collection of nonnegative integers x satisfies the inequalities $x \leq n, x \leq m,$ *and* $n - x \leq N - m$.[xxv]

The details of our sampling strategy[8] are provided in the figures and tables that follow. First is the OC curve, followed by a table of probabilities computed to generate the curve.

Figure 2. HITRUST i1 Rapid Recertification OC Curve



8 Requirements marked as 'not applicable' (N/A) are not included in the sample(s).

Table 1. HITRUST i1 Rapid Recertification Sampling Plan – OC Curve Probabilities

Number Defective (D) in the Lot	Percent Defective in the Lot	Single Sample Accept.	Single Sample Accept. %,	Case I			Case II			Prob. Of Accept. AT Second Sample	Combined Prob. Of Accept.	% Combined Prob. Of Accept.
				First Sample, d=3	Second Sample, d<=2	Prob. Of Accept,	First Sample, d=4	Second Sample, d<=1	Prob. Of Accept			
0	0.0000	1.0000	100.00	0.0000	1.0000	0.0000	0.0000	1.0000	0.0000	0.0000	1.0000	100.0000
1	0.0055	1.0000	100.00	0.0000	1.0000	0.0000	0.0000	1.0000	0.0000	0.0000	1.0000	100.0000
2	0.0110	1.0000	100.00	0.0000	1.0000	0.0000	0.0000	0.7602	0.0000	0.0000	1.0000	100.0000
3	0.0165	0.9654	96.45	0.0346	0.8841	0.0306	0.0000	0.5124	0.0000	0.0306	0.9960	99.5987
(AQL) 4	**0.0220**	**0.8946**	**89.46**	**0.0944**	**0.7029**	**0.0664**	**0.0110**	**0.3219**	**0.0035**	**0.0699**	**(1 – α) 0.9645**	**96.4479**
5	0.0275	0.7983	79.83	0.1604	0.5156	0.0827	0.0378	0.1927	0.0073	0.0900	0.8883	88.8318
6	0.0330	0.6896	68.96	0.2175	0.3555	0.0773	0.0775	0.1113	0.0086	0.0860	0.7755	77.5513
7	0.0385	0.5792	57.92	0.2574	0.2334	0.0601	0.1233	0.0624	0.0077	0.0678	0.6470	64.7010
8	0.0440	0.4751	47.51	0.2777	0.1472	0.0409	0.1677	0.0342	0.0057	0.0466	0.5217	52.1700
9	0.0495	0.3817	38.17	0.2801	0.0897	0.0251	0.2047	0.0183	0.0037	0.0289	0.4106	41.0607
10	0.0549	0.3013	30.13	0.2683	0.0530	0.0142	0.2307	0.0096	0.0022	0.0164	0.3177	31.7708
11	0.0604	0.2340	23.40	0.2466	0.0305	0.0075	0.2445	0.0050	0.0012	0.0087	0.2427	24.2743
12	0.0659	0.1792	17.92	0.2192	0.0172	0.0038	0.2466	0.0025	0.0006	0.0044	0.1836	18.3573
13	0.0714	0.1355	13.55	0.1894	0.0094	0.0018	0.2389	0.0013	0.0003	0.0021	0.1376	13.7558
(LTPD) 14	**0.0769**	**0.1012**	**10.12**	**0.1598**	**0.0051**	**0.0008**	**0.2236**	**0.0006**	**0.0001**	**0.0010**	**(β) 0.1022**	**10.2178**
15	0.0824	0.0748	7.48	0.1320	0.0027	0.0004	0.2033	0.0003	0.0001	0.0004	0.0752	7.5248
16	0.0879	0.0548	5.48	0.1070	0.0014	0.0001	0.1802	0.0001	0.0000	0.0002	0.0549	5.4947
17	0.0934	0.0397	3.97	0.0853	0.0007	0.0001	0.1561	0.0001	0.0000	0.0001	0.0398	3.9790
18	0.0989	0.0286	2.86	0.0670	0.0004	0.0000	0.1326	0.0000	0.0000	0.0000	0.0286	2.8579
19	0.1044	0.0204	2.04	0.0519	0.0002	0.0000	0.1106	0.0000	0.0000	0.0000	0.0204	2.0366
20	0.1099	0.0144	1.44	0.0397	0.0001	0.0000	0.0908	0.0000	0.0000	0.0000	0.0144	1.4402
21	0.1154	0.0101	1.01	0.0300	0.0000	0.0000	0.0734	0.0000	0.0000	0.0000	0.0101	1.0109
22	0.1209	0.0070	0.70	0.0225	0.0000	0.0000	0.0585	0.0000	0.0000	0.0000	0.0070	0.7045
23	0.1264	0.0049	0.49	0.0166	0.0000	0.0000	0.0460	0.0000	0.0000	0.0000	0.0049	0.4875
24	0.1319	0.0034	0.34	0.0122	0.0000	0.0000	0.0358	0.0000	0.0000	0.0000	0.0034	0.3351
25	0.1374	0.0023	0.23	0.0089	0.0000	0.0000	0.0275	0.0000	0.0000	0.0000	0.0023	0.2288
26	0.1429	0.0016	0.16	0.0064	0.0000	0.0000	0.0209	0.0000	0.0000	0.0000	0.0016	0.1553
27	0.1484	0.0010	0.10	0.0046	0.0000	0.0000	0.0157	0.0000	0.0000	0.0000	0.0010	0.1047
28	0.1538	0.0007	0.07	0.0032	0.0000	0.0000	0.0117	0.0000	0.0000	0.0000	0.0007	0.0701
29	0.1593	0.0005	0.05	0.0023	0.0000	0.0000	0.0087	0.0000	0.0000	0.0000	0.0005	0.0467
30	0.1648	0.0003	0.03	0.0016	0.0000	0.0000	0.0063	0.0000	0.0000	0.0000	0.0003	0.0309

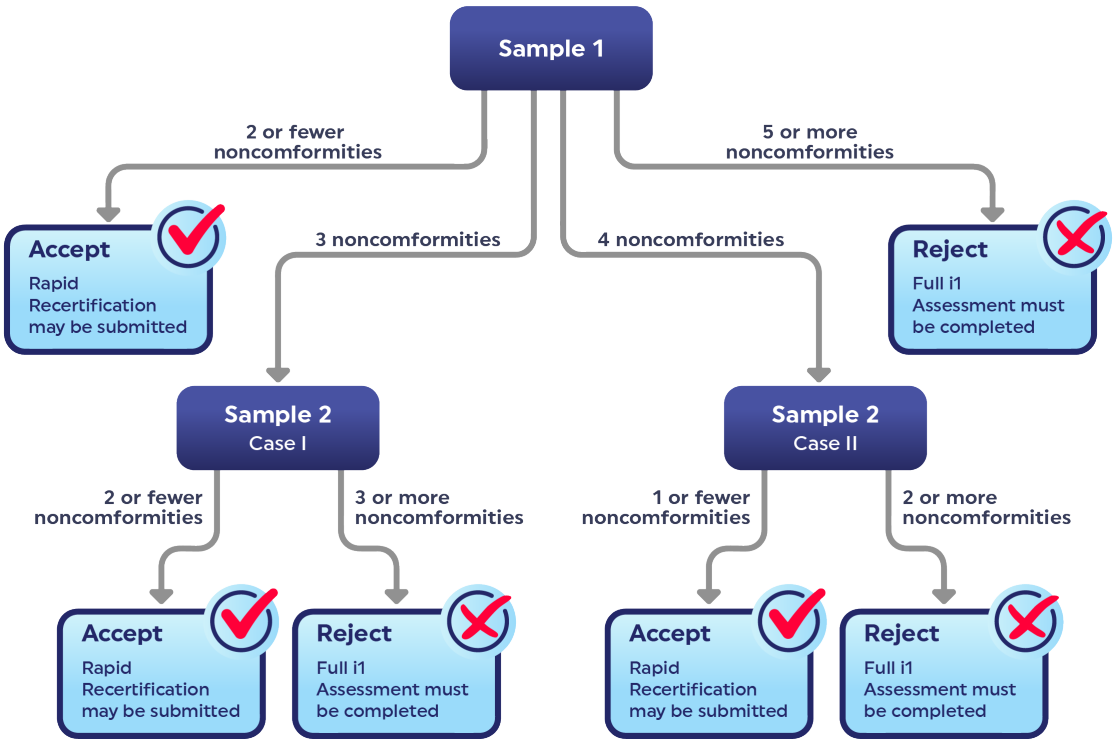
See the table below for the parameters used in the preceding table and in the flow chart that follows.

Table 2. HITRUST i1 Rapid Recertification OC Curve Parameters

Parameter	Value
First Sample Lot Size, N1	182
Second Sample Lot Size, N2	122
First Sample Size, n1	60
Second Sample Size, n2	60
First Sample Accept. Criterion, c1	2
Second Sample Accept. Criterion, c2*	5
First Sample Reject. Criterion, r1	5
Second Sample Reject. Criterion, r2	6

* c2 contains c1

Figure 3. Accept/Reject Decision Flow Chart



Using this approach, we see it is possible to accept an i1 Rapid Assessment in the first random sample of 60 (out of a possible total of 182) i1 requirement statements with 2 or fewer HITRUST i1 requirements scoring less than the original assessment used for certification and rejecting the assessment outright with 5 or more lower scores. For the indeterminate cases when there are 3 or 4 lower scores in the first sample, we conduct a second sample of 60 i1 requirement statements (out of the 122 remaining) and accept the i1 Rapid Assessment if the total number of lower scores from the first and second samples is less than 6 and reject the assessment if there are 6 or more. Regardless of the point in the process where the i1 Rapid Assessment is rejected, a full HITRUST i1 Validated Assessment must be performed by assessing all i1 requirements that were not previously sampled.[9]

9 A complete discussion of the various scenarios addressed by the sampling plan is provided in HITRUST Assurance Advisory (HAA) 2023-005: i1 Rapid Recertification, a link for which is provided in Appendix C.

Departures from the Sampling Plan

Exclusion of Requirements Marked as N/A

HITRUST Policy is to exclude requirements marked as 'N/A' from the sampling frame,[10] which results in a smaller lot size for each stage of the double sampling plan, a lot size of N < 182. To understand the impact of reducing the lot size in this way, let us look at six cases with a fixed AQL = 4 and LTPD = 14 where a specific number of requirements are removed.

Table 3. Impact of N/A'd Requirements on Risk

Parameter	N = 182	N = 177	N = 167	N = 167	N = 162	N = 157	N = 152
α	0.0355	0.0421	0.0500	0.0597	0.0715	0.0859	0.8965
β	0.1022	0.0890	0.0767	0.0652	0.0546	0.0450	0.0363

The preceding table provides values for producer risk, α, and consumer risk, β, for lot sizes between 182 and 152 requirements in decrements of 5 N/A'd requirements.[11] It is clear from the table that, for a fixed AQL and LTPD, the probability of rejecting a good assessment for i1 Rapid Recertification increases as the number of N/A'd items increases while the probability of accepting a bad assessment decreases as the sampling frame becomes smaller.

Given nominal accepted values of α and β in acceptance sampling plans are generally set at 0.05 and 0.10, respectively, and typically range from 0.01 to 0.2,[xxvi] HITRUST believes the observed changes in risk are acceptable.

Inclusion of Requirements with Required CAPs

To maintain visibility into i1 requirements that scored low enough to require a corrective action plan (CAP), HITRUST requires organizations to include i1 requirements which had a CAP in the initial sample of the double sampling plan. A stratified sample[12] like this would not be problematic if the selection of i1 requirements with or without a CAP were random and proportional to their representation in the population. However, HITRUST also requires the first sample in the double sampling plan to include all requirements with a CAP from the i1 Assessment, which makes the 'sub-sample' of these requirements purposive, i.e., non-random,[xxvii] and nonproportional. This could subsequently limit the generalizability of our acceptance sampling plan to the overall population of i1 requirements in an assessment due to sampling bias as the overall sample may not fairly represent the population.

To evaluate the potential impact on generalizability, we note that an i1 Assessment that resulted in HITRUST i1 Certification would likely have no more than ten requirements with a CAP (based on HITRUST i1 Certification requirements). This constitutes less than 5.5% of the 182 requirements in the assessment. If we account for up to 30 requirements marked as N/A, this is still less than 6.6% in the reduced sample frame (N = 152 rather than 182). We subsequently believe the impact to generalizability of the acceptance sampling plan is minimal if not entirely negligible.

Now consider the scenario in which the 10 requirements with a CAP are assessed *a priori*, i.e., before the remaining 50 requirements without a CAP are sampled and assessed. We can subsequently condition the acceptance sampling plan on the number of nonconforming requirements with a CAP

10 A sampling frame is essentially a specific list of all items in the population under study. By removing specific requirements marked as 'N/A' from an assessment of a 'fixed size', i.e., 182 requirements, the number of items that can be sampled for such an assessment is subsequently reduced.

11 In our experience, the number of requirements that can be marked as N/A would likely not exceed 25 or 30 as there are only 23 fully inheritable requirements and a handful of other requirements that could be legitimately marked as such in an i1 assessment.

12 A stratified sample is a one that partitions the sample into smaller groups based on specific characteristics of interest.

found and examine the impact on the plan through the lens of conditional probability.

Let d11 represent the possible number of defective requirements in the first sample, $d11_A$ represent the possible number of defective requirements in the census of all requirements with a CAP in the first sample, and $d11_B$ represent the number of defective requirements in the random sample of requirements without a CAP in the first sample. Then

$$P(d11 \leq X) = P(d11_A + d11_B \leq X) = P[(d11_A = x) \cap (d11_B \leq X - x)] = P(d11_A = x) \cdot P(d11_B \leq X - x)$$

where *X* represents the total actual number of defective requirements with and without a CAP found in the sample d11 and *x* represents the actual number of defective requirements with a CAP in $d11_A$ such that $x < X$. And, since there are *x* number of deficient requirements with a CAP in the assessment, then the probability of finding all x of them in the census of requirements with a CAP is exactly one. Conversely, the probability of finding some other number of deficient requirements with a CAP is exactly zero. As a result,

$$P(d11 \leq X) = P(d11_A = x) \cdot P(d11_B \leq X - x) = 1 \cdot P(d11_B \leq X - x) = P(d11_B \leq X - x)$$

We can now evaluate how the double sampling plan is impacted by a number of known defective requirements with a CAP, x, and evaluating the plan for $0 < x < r1 = 5$, where c1 is the rejection criterion for the first sample.[13] The following table presents the impact of requirements with a CAP on risk for fixed N = 172, n1 = 50, n2 = 60 for $0 < x < 3$, n2 = 0 for $x = 4$, and LTPD = 14. Acceptance and rejection criteria as well as AQL[14] are decremented by the number of defective requirements with a CAP, *x*, found in the census.

Table 4. Impact of Nonconforming CAP'd Requirements on Risk

Plan Type	*x*	n_1	n_2	c_1	r_1	c_2	r_2	AQL[15]	α	β
Double	0	50	60	2	5	5	6	4	0.0246	0.1696
Double	1	50	60	1	4	4	5	3	0.0323	0.0488
Double	2	50	60	0	3	3	4	2	0.0200	0.0068
Double	3	50	60	0	2	2	3	1	0.0000	0.0065
Single	4	50	-	0	1	-	-	0	0.0000	0.0065

Recall that our original double sampling plan, where N = 182 and n1 = n2 = 60, that α = 0.0355 and β = 0.1022. As we can see from the table, the risk of rejecting a good assessment for HITRUST i1 Rapid Certification, α, is less than the risk presented in the original double sampling plan for all permissible nonconforming requirements with a CAP, *x*, and the risk of accepting a bad assessment, β, is also less than the original plan except where one nonconforming requirement with a CAP is found *a priori*. Even so, the value of β = 0.1696 is acceptable since $0.01 < \beta < 0.20$.[xxviii] (Note also that B = 0.1025 for an LTPD of 16 vice 14 nonconforming i1 requirements in the overall assessment.)

Based on this analysis, we believe the practical impact on producer and consumer risk in the modified

13 Note that, once r1 − c1 =1, we necessarily revert back to a single sample acceptance sampling plan.

14 Since a census of i1 assessment requirements with a CAP with 5 or more defectives necessarily forces rejection of the lot before any of the randomly selected requirements are considered, we can evaluate performance of the acceptance sampling plan by considering values of $X = 0, 1, 2, 3$, and 4 defectives in the census of requirements with a CAP in conjunction with a random sample of 50 i1 requirements without a CAP. If there are 5 defective requirements with a CAP, the entire sample is rejected and the assessment is not qualified for i1 Rapid Recertification.

15 AQL suggests that a lot can be accepted if the number of nonconformities found is less than or equal to the acceptance number, α; we subsequently chose to decrement AQL by the number of nonconformities found in the census of requirements with a CAP and provide the producer risk, α, for that value.

double sampling plan is acceptable.

Final Thoughts

The LASP articulated in this paper provides an AQL ≈ 4 nonconforming controls (2.2%), which translates to an approximate 3.5% probability of requiring a full i1 Validated Assessment for recertification when Rapid Certification would have otherwise been acceptable. It also provides an LTPD ≈ 14 nonconforming controls (17%), which means there is an approximate 10% chance of approving an i1 Rapid Recertification when 14 or more controls may have degraded from the time they were initially assessed for certification. Further inspection of the probabilities in the OC curve for the sampling plan indicates there is only a 3.1% likelihood that Rapid Recertification would be approved when 30 controls (16.5%) may have degraded. And, by sampling a minimum of a third of the controls in an i1 Validated Assessment,[16] this approach to i1 Rapid Recertification balances the need for a suitable amount of 'inspection' to support the assurance requirements of relying parties with the reduced cost, time, and effort[17] required for recertification desired by Assessed Entities.

16 This is consistent with an approach to the reauthorization of U.S. government information systems in which a third of the controls are assessed every three years so that all controls are assessed within a three-year reauthorization period.

17 Assessing a third of the controls means a reduction of as much as one-third of the variable costs associated with an assessment (per control) and potentially a slight reduction in fixed costs (overhead) attributed to the assessment.

About the Authors

Bryan Cline, Ph.D., Chief Research Officer

Bryan provides thought leadership on risk management and compliance and develops the methodologies used in various components of the HITRUST Approach. This includes a focus on the design of the HITRUST CSF and the assessment and certification models used in the HITRUST Assurance Program, for which he provides technical direction and oversight. He is also responsible for addressing emerging trends impacting risk management and compliance to ensure the HITRUST Approach sets the bar for organizations seeking the most comprehensive privacy and security frameworks available. Bryan previously served as HITRUST's Vice President of Standards and Analysis.

Bimal Sheth, EVP Standards Development and Assurance Operations

Bimal leads the development of the HITRUST CSF and Assurance program. His teams are responsible for conducting research of information protection practices, enhancing the HITRUST CSF by incorporating new or updated authoritative sources, ensuring the Rely-Ability of HITRUST Certifications, and educating the HITRUST community about the CSF through training. Bimal has spent his career working with organizations to provide assurances over their information protection programs.

About HITRUST

Since it was founded in 2007, HITRUST has championed programs that safeguard sensitive information and manage information risk for global organizations across all industries and throughout the third-party supply chain. In collaboration with privacy, information security and risk management leaders from the public and private sectors, HITRUST develops, maintains, and provides broad access to its widely adopted common risk and compliance management frameworks, related assessments and assurance methodologies. The HITRUST Approach provides organizations a comprehensive information risk management and compliance program to provide an integrated approach that ensures all programs are aligned, maintained, and comprehensive.

Figure 4. The HITRUST Approach

HITRUST also actively participates in many efforts in government advocacy, community building, and cybersecurity education. For more information, visit www.hitrustalliance.net.

Appendix A – Acronyms and Abbreviations

Accept.	Acceptance
AQL	Acceptable Quality Limit (or Level)
c	Acceptance Criterion
d	Defect (or Nonconformity)
LASP	Lot Acceptance Sampling Plan
LTPD	Lot Tolerance Percent Defective
N	Population Size
n	Sample Size
OC	Operating Characteristic
Prob.	Probability
r	Rejection Criterion
Reject.	Rejection
SP	Sampling Plan
X	Number of Nonconformities
α	Producer Risk
β	Consumer Risk

Appendix B – Glossary of Terms

Acceptable Quality Limit (or Level)	A number/percentage of nonconformities that defines a minimum level of quality for the product or service.
Acceptance Sampling	A statistical method of quality control that involves testing a sample of products or services to determine the overall quality of the batch from which the sample is derived.
Acceptance Sampling Plan	See Lot Acceptance Sampling Plan
Assurance	Grounds for justified confidence that a claim has been or will be achieved.
Batch	See Lot
Consumer	The entity receiving the product or service represented in a lot. In our use case, it is essentially the relying party.
Consumer Risk	Signified as β, it is the probability of accepting a lot with an otherwise unacceptable quality level (number or percentage of nonconformities).
Defect	See Nonconformity
Double Sampling Plan	A sampling plan in which a second sample may be taken and the results combined with the first sample if the results from the first sample are inconclusive.
Generalizability	The ability to extend research findings and conclusions drawn from an analysis of a sample to the overall population from which it is drawn. Generalizability is typically determined by how well a sample is representative of the population. Synonymous with external validity.
HITRUST i1 (Validated) Assessment	Assessment of a static set of best/leading practice HITRUST CSF controls by an External Assessor, the results of which are reviewed under the HITRUST quality assurance process.
HITRUST i1 Certification	A HITRUST i1 Validated Assessment that meets a minimum set of HITRUST-defined scoring criteria.
Hypergeometric Distribution	A type of probability distribution that describes the chance of getting a certain number of successes in a sample drawn from a finite population, without putting the items back after each draw. It is similar to the binomial distribution, but the probability of success changes after each draw because the population size decreases.
Lot	A collection of items (products or services) that are assumed to have uniform quality characteristics.

Lot Acceptance Sampling Plan	A sampling and binary decision-making scheme around the acceptability (quality) of a product or service.
Lot Size	The number of distinct elements (product or service) contained in a lot.
Lot Tolerance Percent Defective	A percentage of nonconformities that would be unacceptable to a consumer.
Multiple Sampling Plan	A sampling plan in which more than two samples may be needed to reach a conclusion.
Nonconformity	See Defect
Operating Characteristic	Specific attributes or parameters of an acceptance plan (e.g., N, n, c, and r).
Operating Characteristic Curve	A plot of the probability of accepting a lot (Y-axis) versus a number, lot fraction, or percent defectives (X-axis).
Population	A complete group of items or entities that share defined characteristics.
Probability Distribution	A statistical function that describes the likelihood of obtaining all possible values a specific random variable can take.
Probability Distribution Function	A general term that describes the probabilities of different possible outcomes for any type of random variable, whether it is discrete or continuous.
Probability Mass Function	A type of probability distribution function that only applies to discrete random variables, which are random variables that can take only a finite or countable number of values and give the probability the variable is exactly equal to a specific value.
Producer	The entity providing the product or service contained in a lot. In our use case, it is the External Assessor and Assessed Entity.
Producer Risk	Signified as α, it is the probability of rejecting a lot with an otherwise acceptable quality level (number or percentage of nonconformities).
Quality Assurance	A proactive process of ensuring quality standards or certifications are met throughout the entire production or service delivery process.
Quality Control	A reactive process performed to ensure products or services produced or delivered by an entity meet certain quality standards or specifications.
Rely-Ability	The ability of a stakeholder to rely upon [i.e., trust or have confidence in] the assurances provided by an entity.

Sample	A subset of items or entities drawn from a population.
Sample Size	The number of items or entities drawn from a population.
Sampling Plan	See Lot Acceptance Sampling Plan
Sequential Sampling Plan	A sampling plan in which the number of samples is equivalent to the number of items in the lot.
Single Sampling Plan	A sampling plan in which a single sample is taken and a determination is made based on the number of nonconformities in the sample.
Skip Lot Sampling Plan	A sampling plan in which only a fraction of the submitted lots is inspected.
Stratified (Random) Sample	A statistical sample obtained by partitioning a population into relatively homogeneous strata based on common characteristics of interest to a researcher. A subsample is randomly drawn from each stratum in proportion to their representation in the overall population, which allows research to draw conclusions for each subpopulation.
Threat-Adaptive	Refers to a HITRUST Assessment that leverages continuously updated threat intelligence and integrates best practices intended to help protect entities against evolving cyber threats.
Type I Error	See Producer Risk
Type II Error	See Consumer Risk

Appendix C – Reference List

Bennekers, V. (Ed.) (2023, Sep). HITRUST Assessment Handbook. Frisco, TX: HITRUST. Available from https://hitrustalliance.net/manual/.

Cline, B. (2023, Sep). The HITRUST Risk Management Handbook: A discussion of framework-based risk analysis and control specification, implementation, assessment, and reporting for HITRUST Organizations and Assessors. Frisco, TX: HITRUST. Available from https://hitrustalliance.net/manual-risk-management/.

Cline, B., Huval, J., and Sheth, B. (2020, Sep). Evaluating Control Maturity Using the HITRUST Approach: Quasi-quantitative scoring based on the HITRUST CSF security and privacy control implementation maturity model. Available from https://hitrustalliance.net/content/uploads/Evaluating-Control-Maturity-Using-the-HITRUST-Approach.pdf.

HITRUST (2023a). HITRUST CSF. Available from https://hitrustalliance.net/product-tool/hitrust-csf/.

HITRUST (2023b). HITRUST Assurance Program. Available from https://hitrustalliance.net/hitrust-assurance-program/.

HITRUST (2023c). HITRUST Implemented, 1-Year (i1) Validated Assessment. Available from https://hitrustalliance.net/certification/hitrust-implemented-1-year-i1-validated-assessment/.

HITRUST (2023d). HITRUST Essentials, 1-year (e1) Validated Assessment. Available from https://hitrustalliance.net/certification/hitrust-essentials-1-year-e1-validated-assessment/.

HITRUST (2023e). HITRUST Risk-based, 2-year (r2) Validated Assessment. Available from https://hitrustalliance.net/certification/hitrust-risk-based-2-year-r2-validated-assessment/.

ITRUST (2023f). Getting Started with HITRUST. Available from https://info.hitrustalliance.net/fy23-getting-started-with-hitrust.

HITRUST (2023g). External Assessors. Available from https://hitrustalliance.net/assessor/external-assessors/.

HITRUST (2023h). HAA 2023-005: i1 Rapid Recertification. Available from https://hitrustalliance.net/advisories/#haa2023-005.

HITRUST (2023i). MyCSF – Our SaaS Platform. Available from https://hitrustalliance.net/product-tool/mycsf/.

HITRUST (2023j). HITRUST Results Distribution System. Available from https://hitrustalliance.net/results-distribution-system/.

HITRUSTAX (2023). Streamlining the Process of Third-Party Risk Management (TPRM). Available from https://hitrustax.com/.

NIST (2023). Dataplot: Vol 2: Single Sample Acceptance Plan. Available from https://www.itl.nist.gov/div898/software/dataplot/refman1/auxillar/singsamp.htm.

NIST/SEMATECH (2023a). e-Handbook of Statistical Methods: 6.1.1. How did statistical quality control begin? Available from https://www.itl.nist.gov/div898/handbook/pmc/section1/pmc11.htm.

NIST/SEMATECH (2023b). e-Handbook of Statistical Methods: 6.2.1. What is acceptance sampling? Available from https://www.itl.nist.gov/div898/handbook/pmc/section2/pmc21.htm.

NIST/SEMATECH (2023c). e-Handbook of Statistical Methods: 6.2.2. What kinds of lot acceptance sampling plans are there? Available from https://www.itl.nist.gov/div898/handbook/pmc/section2/pmc22.htm.

NIST/SEMATECH (2023d). e-Handbook of Statistical Methods: 3.4.5. Assessing Process Stability. Available from https://www.itl.nist.gov/div898/handbook/ppc/section4/ppc45.htm.

NIST/SEMATECH (2023e). e-Handbook of Statistical Methods: 6.1.6. What is process capability? Available from https://www.itl.nist.gov/div898/handbook/pmc/section1/pmc16.htm.

Samohyl, R. (2017, Oct 7). Acceptance sampling for attributes via hypothesis testing and the hypergeometric distribution. Journal of Industrial Engineering International, 14, p. 395. Available from https://link.springer.com/content/pdf/10.1007/s40092-017-0231-9.pdf.

Siegrist, K. (2022, Apr 24). 12.2: The hypergeometric distribution. Available from https://stats.libretexts.org/Bookshelves/Probability_Theory/Probability_Mathematical_Statistics_and_Stochastic_Processes_(Siegrist)/12%3A_Finite_Sampling_Models/12.02%3A_The_Hypergeometric_Distribution.

Appendix D – Endnotes

i HITRUST (2023a). External Assessors. Available from https://hitrustalliance.net/assessor/external-assessors/.

ii HITRUST (2023b). HITRUST CSF. Available from https://hitrustalliance.net/product-tool/hitrust-csf/.

iii HITRUST (2023c). HITRUST Assurance Program. Available from https://hitrustalliance.net/hitrust-assurance-program/.

iv Cline, B. (2023, Sep). The HITRUST Risk Management Handbook: A discussion of framework-based risk analysis and control specification, implementation, assessment, and reporting for HITRUST Organizations and Assessors. Frisco, TX: HITRUST. Available from https://hitrustalliance.net/manual-risk-management/.

v HITRUST (2023d). HITRUST Implemented, 1-Year (i1) Validated Assessment. Available from https://hitrustalliance.net/certification/hitrust-implemented-1-year-i1-validated-assessment/.

vi Cline, B. (2023, Sep).

vii HITRUST (2023e). HITRUST Essentials, 1-year (e1) Validated Assessment. Available from https://hitrustalliance.net/certification/hitrust-essentials-1-year-e1-validated-assessment/.

viii HITRUST (2023f). HITRUST Risk-based, 2-year (r2) Validated Assessment. Available from https://hitrustalliance.net/certification/hitrust-risk-based-2-year-r2-validated-assessment/.

ix HITRUST (2023d).

x HITRUST (2023g). Getting Started with HITRUST. Available from https://info.hitrustalliance.net/fy23-getting-started-with-hitrust.

xi HITRUST (2023h). HAA 2023-005: i1 Rapid Recertification. Available from https://hitrustalliance.net/advisories/#haa2023-005.

xii Ibid.

xiii HITRUST (2023i). MyCSF – Our SaaS Platform. Available from https://hitrustalliance.net/product-tool/mycsf/.

xiv Cline, B., Huval, J., and Sheth, B. (2020, Sep). Evaluating Control Maturity Using the HITRUST Approach: Quasi-quantitative scoring based on the HITRUST CSF security and privacy control implementation maturity model. Available from https://hitrustalliance.net/content/uploads/Evaluating-Control-Maturity-Using-the-HITRUST-Approach.pdf.

xv HITRUSTAX (2023). Streamlining the Process of Third-Party Risk Management (TPRM). Available from https://hitrustax.com/.

xvi HITRUST (2023j). HITRUST Results Distribution System. Available from https://hitrustalliance.net/results-distribution-system/.

xvii NIST/SEMATECH (2023a). e-Handbook of Statistical Methods: 6.1.1. How did statistical quality control begin? Available from https://www.itl.nist.gov/div898/handbook/pmc/section1/pmc11.htm.

xviii NIST/SEMATECH (2023b). e-Handbook of Statistical Methods: 6.2.1. What is acceptance sampling? Available from https://www.itl.nist.gov/div898/handbook/pmc/section2/pmc21.htm.

xix NIST/SEMATECH (2023c). e-Handbook of Statistical Methods: 6.2.2. What kinds of lot acceptance sampling plans are there? Available from https://www.itl.nist.gov/div898/handbook/pmc/section2/pmc22.htm.

xx Ibid.

xxi Bennekers, V. (Ed.) (2023, Sep). HITRUST Assessment Handbook. Frisco, TX: HITRUST. Available from https://hitrustalliance.net/manual/.

xxii NIST/SEMATECH (2023d). e-Handbook of Statistical Methods: 3.4.5. Assessing Process Stability. Available from https://www.itl.nist.gov/div898/handbook/ppc/section4/ppc45.htm.

xxiii NIST/SEMATECH (2023e). e-Handbook of Statistical Methods: 6.1.6. What is process capability? Available from https://www.itl.nist.gov/div898/handbook/pmc/section1/pmc16.htm.

xxiv Samohyl, R. (2017, Oct 7). Acceptance sampling for attributes via hypothesis testing and the hypergeometric distribution. Journal of Industrial Engineering International, 14, p. 395. Available from https://link.springer.com/content/pdf/10.1007/s40092-017-0231-9.pdf.

xxv Siegrist, K. (2022, Apr 24). The hypergeometric distribution. Available from https://stats.libretexts.org/Bookshelves/ Probability_Theory/Probability_Mathematical_Statistics_and_Stochastic_Processes_(Siegrist)/12%3A_Finite_Sampling_Models/12.02%3A_The_Hypergeometric_Distribution.

xxvi NIST (2023). Dataplot: Vol 2: Single Sample Acceptance Plan. Available from https://www.itl.nist.gov/div898/software/dataplot/refman1/auxillar/singsamp.htm.

xxvii NIST/SEMATECH (2023b)

xxviii NIST (2023).