Aprio

OSTENDIO



HITRUST i1 vs. r2:

A Closer Look into the Control Requirements

Aprio

OSTENDIO

At a glance

- **The main takeaway:** HITRUST offers two assessment options for organizations to demonstrate that they store and protect sensitive data with different degrees of requirements. In this article, we take a closer look at HITRUST i1 vs. r2 and compare the control requirements.
- **Impact on your business:** While less requirements may seem appealing, it may be more time consuming on the backend. It's still important to connect with a HITRUST advisor to fully understand the differences between the two assessments and to avoid costly mistakes.
- **Next steps:** Aprio's Information Assurance team and Ostendio's HITRUST team can help you determine the best HITRUST approach to meet the needs of both you and your customers.

The Full Story

Since HITRUST added the additional assessment option, some have suggested that the leaner HITRUST to implement is the 1-Year (i1) assessment, which offers less control requirements, and thus, quicker results than the comprehensive and customizable HITRUST Risk-Based, 2-year (r2) assessment.

While both assessments deliver exceptional risk management, it's helpful to consider a high-level comparison of the i1 and r2 to fully understand the requirement differences.



Aprio

OSTENDIO

Comparing HITRUST i1 to HITRUST r2

HITRUST i1

- Must be performed yearly
- Requires evidence of implementation only
- Organization is assessed based on implementation evidence only
- 219 controls, regardless of scope
- Evidence required only for 219 individual instances
- Auditor cost is lower, but paid annually
- Competitor to SOC 2, which has less requirements for policy and procedure documentation, and is performed every year
- Provides a “one-size-fits-all” moderate assurance level

HITRUST r2

- Must be performed every 2 years with a brief “interim” assessment in the off year
- Requires evidence of policies, procedures and implementation
- Organization is assessed based on a combination of policy quality, procedure quality and implementation evidence
- 230 up to potentially 3,000 controls depending on the scope
- Evidence required for each individual control statement
- Auditor cost is higher every other year and lower on the “interim” year
- Higher regard due to industry perception and considered more rigorous and robust than both SOC 2 and i1
- Controls are customized based on the scoping factors

Aprio

OSTENDIO

While there are several differences between the i1 and r2, the largest variation involves the number of control requirements.

On average, a smaller scope r2 assessment will have between 250 to 350 controls, whereas the i1 has only 219 controls. This difference means that the organization only needs to produce "evidence" 219 times, which on the surface is considerably less than the 250 to 350 controls for the r2. However, the evidence required for those 219 controls may be more difficult and time consuming to implement or provide to your assessor.

This discrepancy is due to the flexibility of scoping in an r2, where requirement statements can be level 1, 2, or 3, with the control requirements building on each other with each level. A small r2 assessment will typically cover mostly level 1 requirements and not reach level 2 or level 3 requirements. However, the i1 assessment incorporates level 2 and level 3 requirements into most of the 219 controls.

Outlined below are examples in which the i1 requires more control statements than the r2.

Example 1: Domain 2 – Endpoint Protection

Under the domain 2 endpoint protection, the i1 assessment has 8 control requirements, whereas a smaller scope r2 assessment only requires 5 control requirements.

The first 2 control statements (shown right) are common to both the i1 and r2.

0201.09j1Organizational.124
Anti-virus and anti-spyware are installed, operating and updated on all end-user devices to conduct periodic scans of systems to identify and remove unauthorized software.

0202.09j1Organizational.3
Audit logs of the scans are maintained.

The 6 control statements below are included in the i1 assessment, but not normally in the r2.

0207.09j2Organizational.56
Centrally managed, up-to-date anti-spam and anti-malware protection is implemented at information system entry/exit points on all devices.

0208.09j2Organizational.7
User functionality is separated from information system management functionality.

0217.09j2Organizational.10
The organization configures, blocks and alerts the administrator of any malicious code and performs real-time scans of information and network entry/exit points.

0221.09jFTIOrganizational.1
The organization requires governing the installation of software by users; enforces software installation restrictions through automated methods; and monitors compliance on a continual basis.

0227.09k2Organizational.12
The organization takes specific action to protect against mobile code performing unauthorized actions.

0231.09jCISOrganizational.7
The organization implements the Sender Policy Framework (SPF) by deploying SPF records in DNS and enabling receiver-side verification in mail servers.

Aprio

OSTENDIO

Of the controls listed above, 207 through 231 are not typically included in the r2 assessment unless the assessment is over 500 controls.

There has been discussion that r2 controls have been removed from the i1, however, the 3 controls (in the table below) have not been removed. In fact, they are included within the new 0201 evaluative elements in the i1. To make matters a bit more complicated, an additional 13 individual sub-requirements — 0214, 0225, 0226 and beyond — are now included in control 0201 in the i1 as evaluative elements. In many cases, controls have not been removed, they have simply been consolidated under broader control statements as evaluative elements that are required to be tested.

0214.09j1Organization.6
Protection against malicious code detection and repair software, security awareness and appropriate system access.

0225.09k1Organizational.1
Automated controls are in place to authorize and restrict the use of mobile code.

0226.09k1Organizational.2
The organization has implemented and regularly updates mobile code protection, including anti-virus and anti-spyware.

Example 2: Some policies remain in the i1

Password management is still required under the i1 assessment, and the specific control statement, outlined below, is more prescriptive than the r2 assessment. The i1 requirement for 1022 still requires documented password policies whereas the r2 requirement for the 1022 is less specific, which provides more ambiguity and flexibility in how to demonstrate the control.

0201.09j1Organizational.124
Password policies applicable to mobile devices are documented and enforced through technical controls on all company devices or devices approved for BYOD usage and prohibit the changing of password/PIN lengths and authentication requirements.

These two examples illustrate the need to understand the nuances of your organization's situation to understand the impact of i1 versus r2.

The bottom line

At first glance, it appears that the i1 will have a smaller scope and smoother implementation process than the r2. However, you shouldn't assume that is the case without fully exploring the control requirements and related evaluative elements for your specific assessment. It's important to connect with a HITRUST advisor at Aprio or Ostendio to better understand your options. Aprio's Information Assurance team and Ostendio's HITRUST team can help you determine the best HITRUST approach to meet the needs for both you and your customer.

Related Resources from Aprio

- About Aprio's HITRUST CSF Services and Compliance
- New HITRUST Reporting Options Aim to Fill Major Gaps in the Market
- Healthcare IT and HIPAA Compliance: Choosing the Right Level Information Risk Management

---

Related Resources from Ostendio

- HITRUST Certification: Is It Right For Your Organization?
- HITRUST Cheat Sheet: How to Choose Your HITRUST Preparer

Aprio



OSTENDIO

Schedule a consultation today with one of Aprio's Information Assurance advisors and an Ostendio HITRUST Consultant.

GET STARTED

APRIO, the Aprio pentagonal pinwheel logo and "PASSIONATE FOR WHAT'S NEXT", are registered marks of Aprio, LLP. Aprio, LLP © 2017-23. All rights reserved.