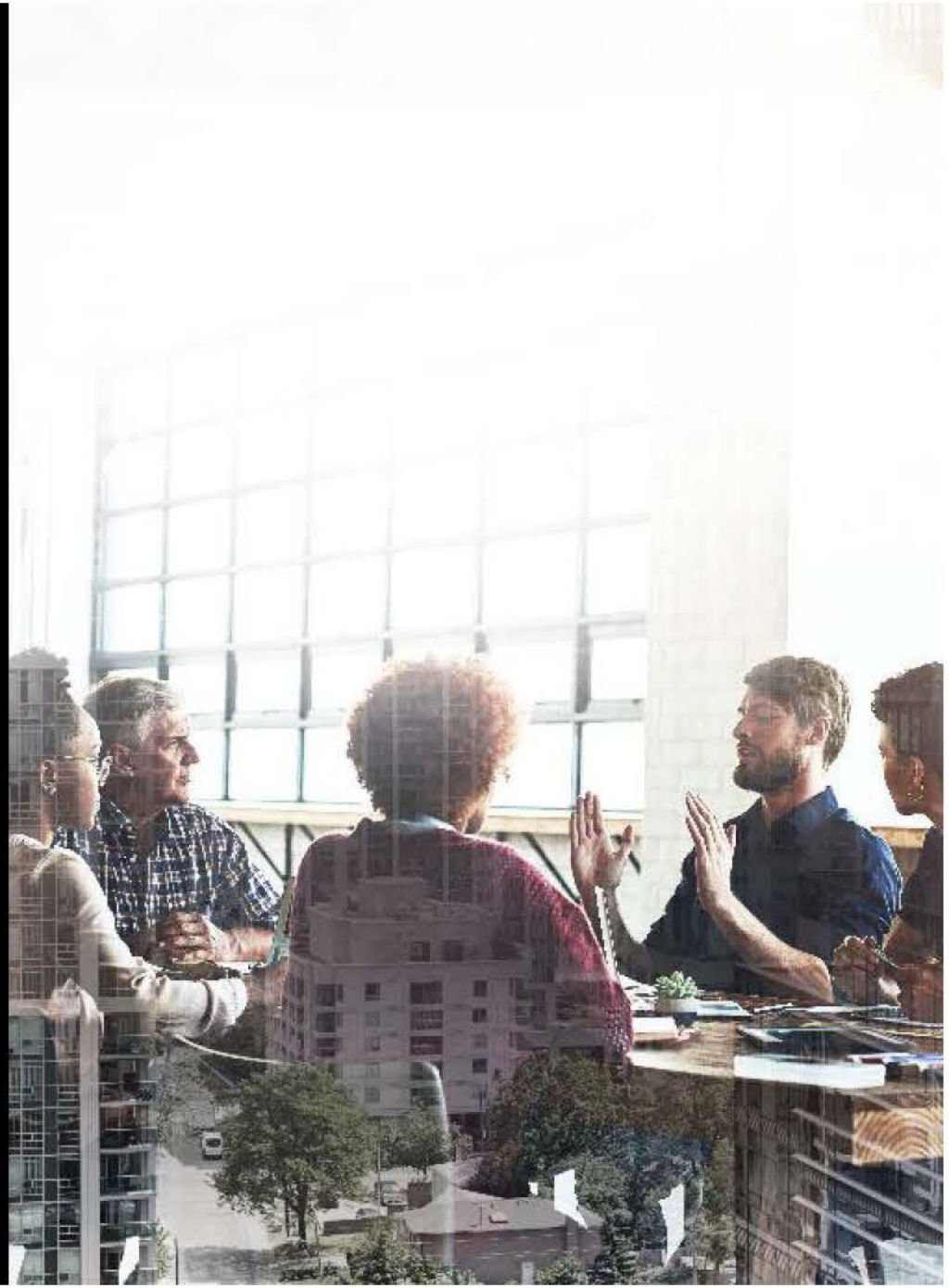
Demystifying HITRUST assessment types: bC, i1 and r2

Which level of assurance should you be requesting or pursuing?

March 2, 2022

bakertilly



Current business needs and challenges

Challenges and questions

What is the difference between these information protection assurances? Which will satisfy my requirements?

How do I know how much assurance my organization needs?

Which HITRUST assessment type should I choose?

What types of compliance efforts should I provide to my clients? Each is asking for something different.

Why the need for quality information protection assurance?

The landscape of information protection assessments

Produces varying levels of assurance, based on…

- Suitability of information protection controls
- Rigor of assessment approach and assurance program

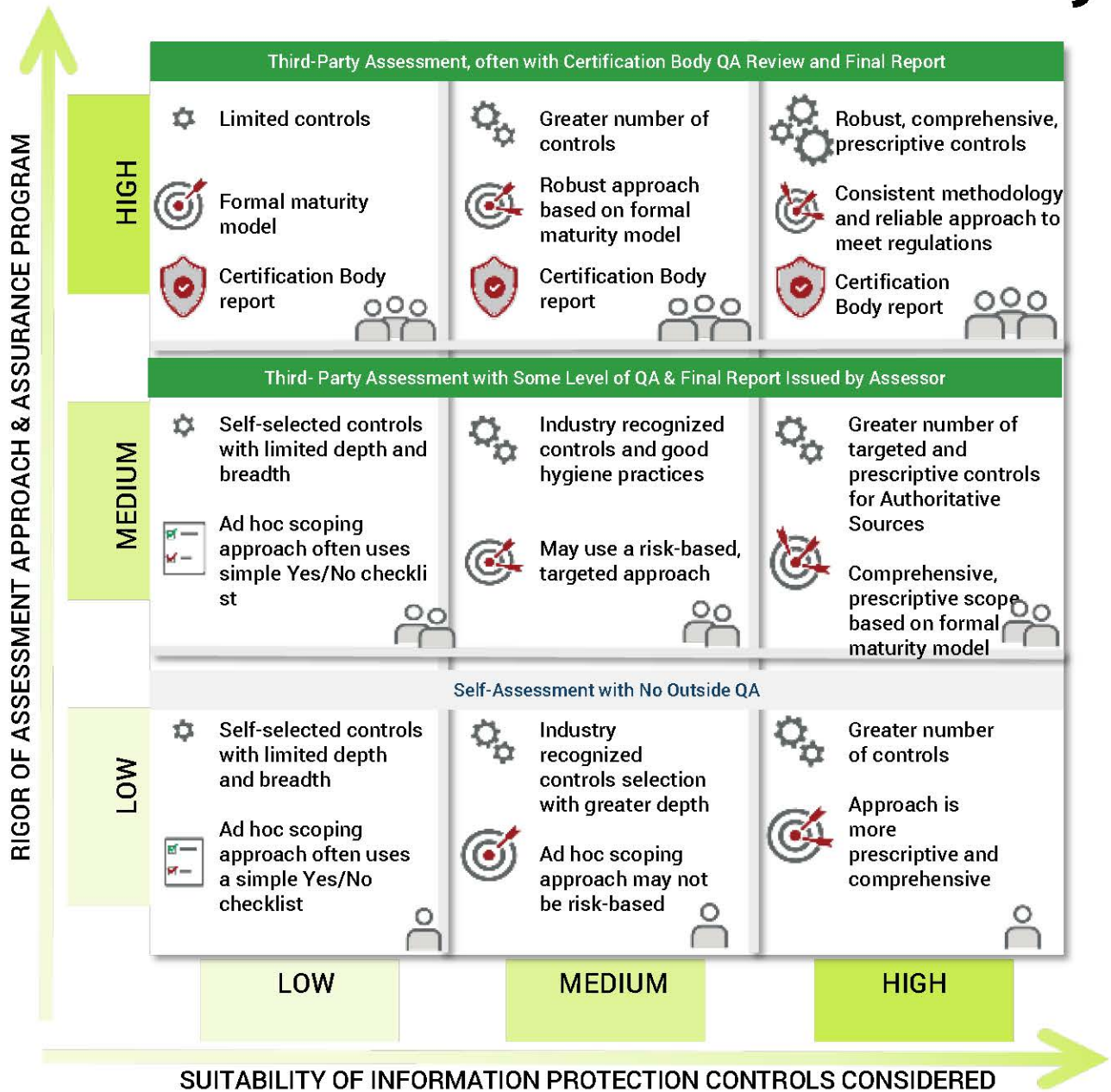
KEY

Level of Controls:

Approach:

Certification Body Report:

Impartiality:
QA & Review:
Self.....
Self & Assessor.....
Self/Assessor/Cert Body.....

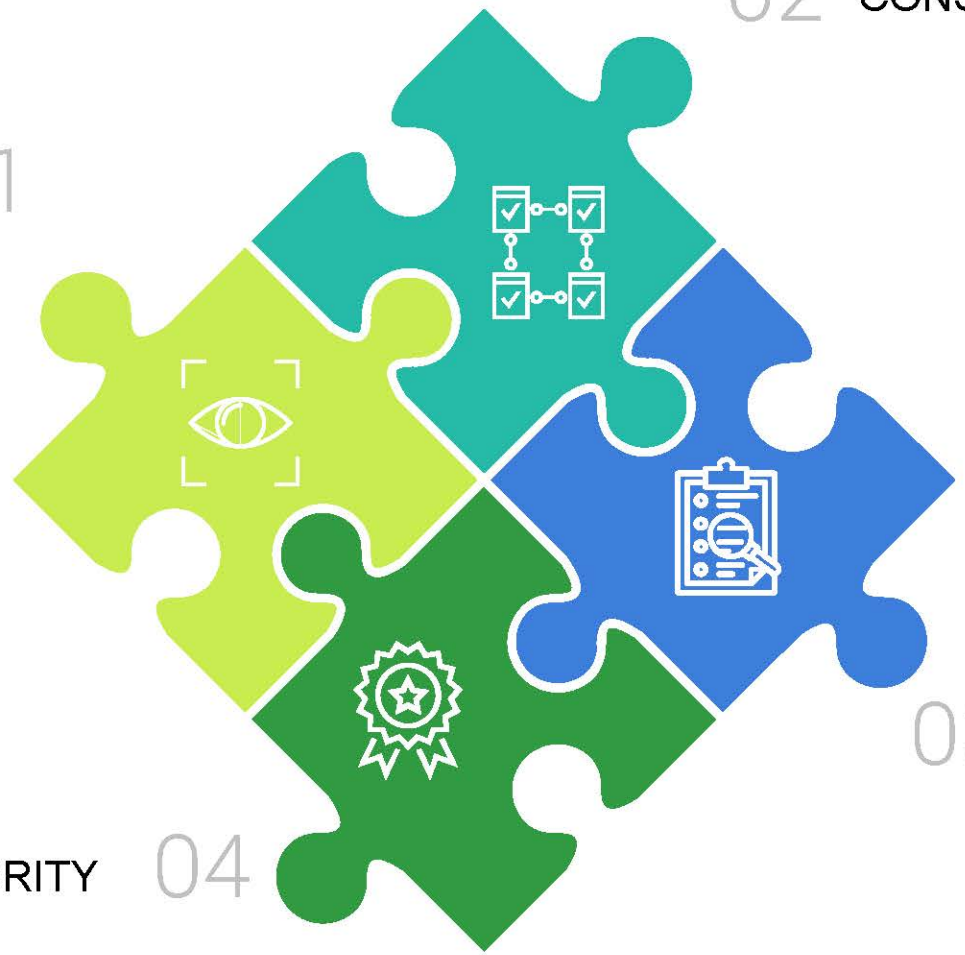


© 2021 HITRUST Alliance

Not all assurances are created equal

01 TRANSPARENCY

02 CONSISTENCY



03 ACCURACY

04 INTEGRITY

Use cases

Use cases

New market entrant

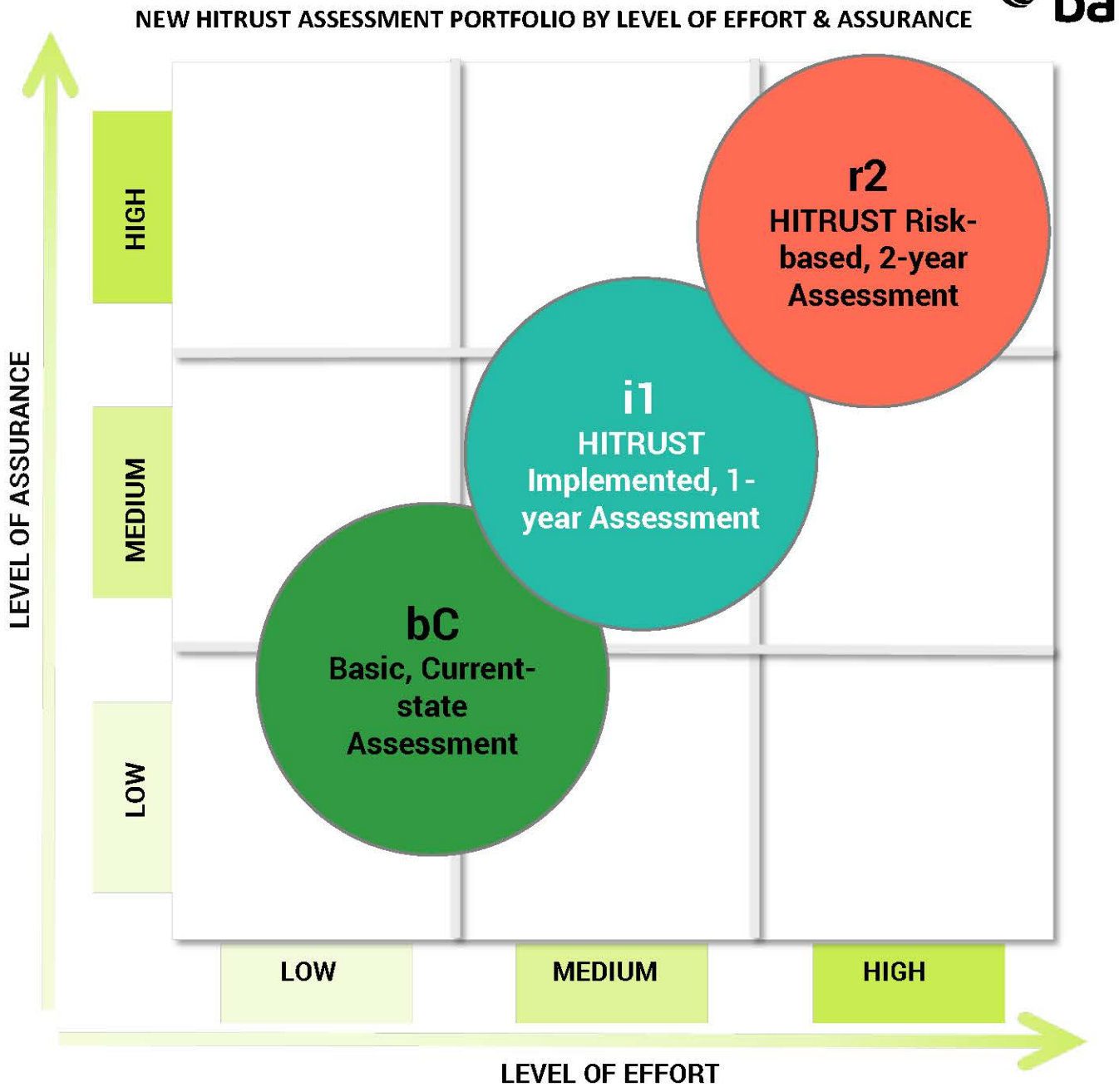
Higher education

Healthcare provider

NEW HITRUST Portfolio options

The growing need for quality low and moderate assurances

- Driven by considerations of purpose, time, and budget
- Current mechanisms on the market have gaps, deficiencies, and inefficiencies that impact their reliability and usefulness
  - Transparency of control requirements
  - Consistency of evidence review
  - Integrity of the process
- HITRUST has introduced two additional assessment options to raise the bar on quality across all levels of assurance with commensurate level of effort



© 2021 HITRUST Alliance

Expanded HITRUST Assessment Portfolio

Basic, Current-state (“bC”) Assessment

Focus on good security hygiene controls in virtually any size organization with a simple approach to evaluation, which is suitable for rapid and/or low assurance requirements

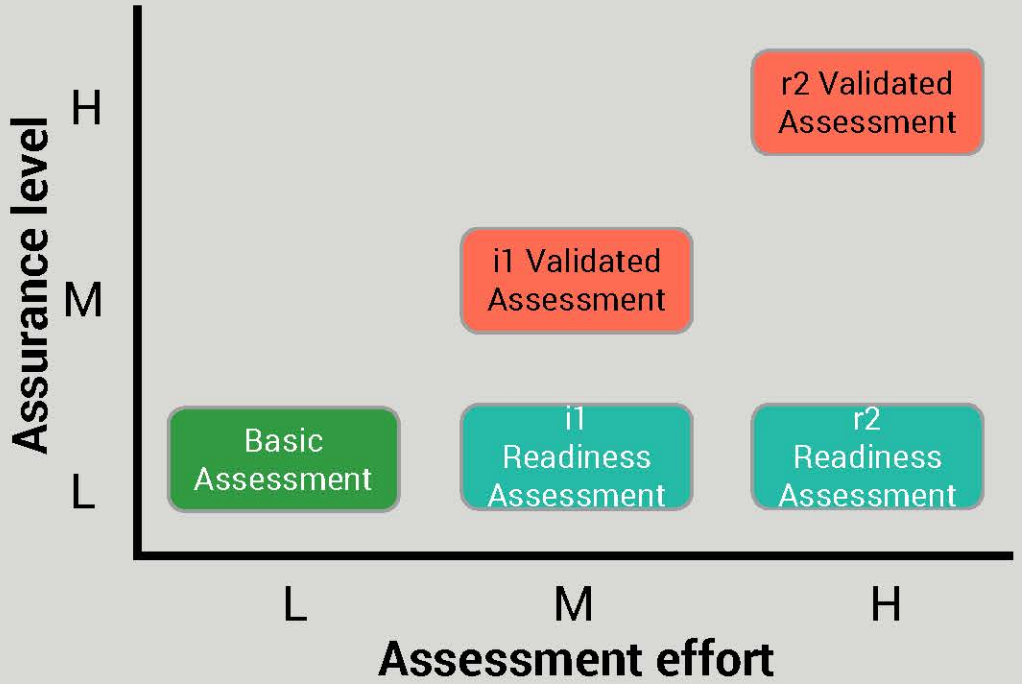
Implemented, 1-year (“i1”) Assessment

Focus on leading security practices with a more rigorous approach to evaluation, which is suitable for moderate assurance requirements

Risk-based, 2-year (“r2”) Assessment

Renames our current “validated assessment”, otherwise unchanged

Focus on a comprehensive risk-based specification of controls with a very rigorous approach to evaluation, which is suitable for high assurance requirement



© 2021 HITRUST Alliance

Expanded HITRUST Assessment Portfolio

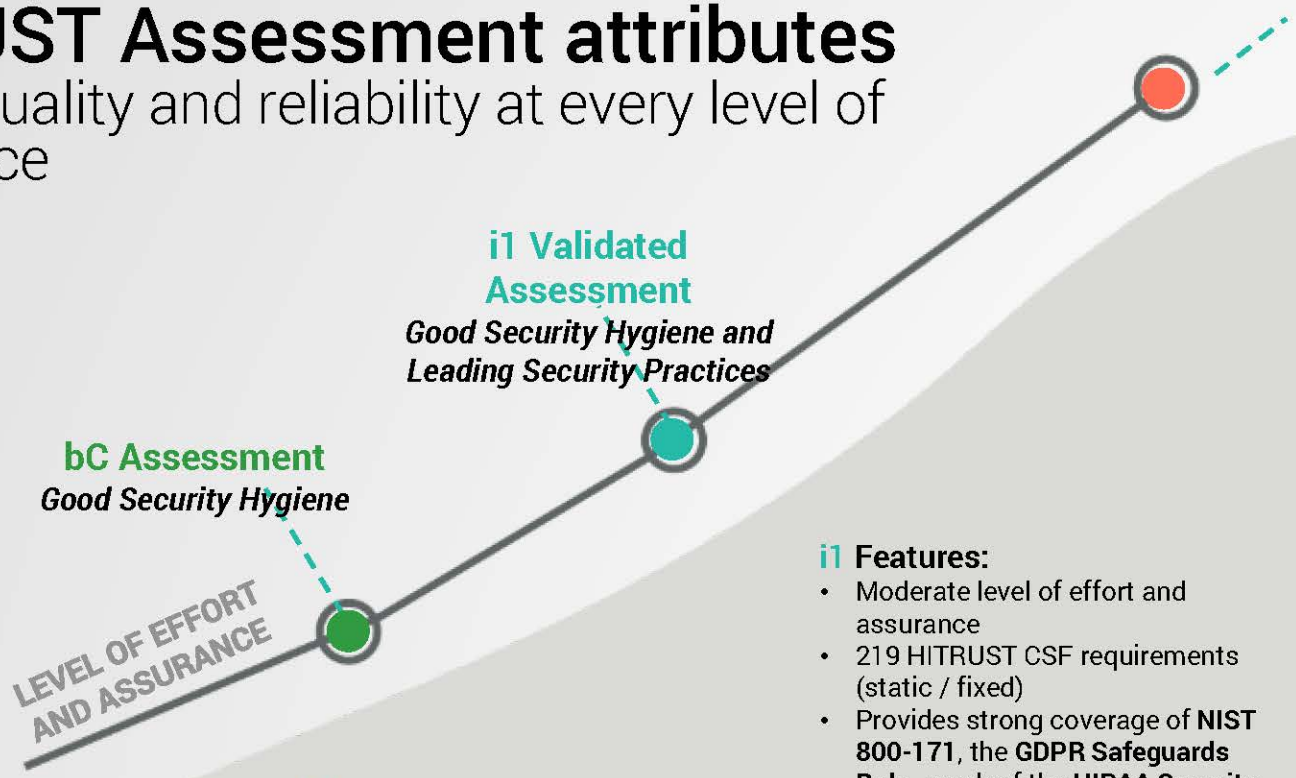
bakertilly

© 2021 HITRUST Alliance

	HITRUST CSF Basic, Current-State Assessment (bC) *(NEW)*	HITRUST CSF Implemented, 1-year (i1) Assessment *(NEW)*	HITRUST CSF Risk-based, 2-year (r2) Assessment *(Former Name: HITRUST CSF Validated Assessment)*
Description	Verified Self-Assessment	Validated Assessment + Certification	Validated Assessment + Risk-Based Certification
Purpose (Use Case)	Focus on good security hygiene controls with a simple approach to evaluation, which is suitable for rapid and/or low assurance requirements	Focus on leading security practices with a more rigorous approach to evaluation, which is suitable for moderate assurance requirements	Focus on a comprehensive risk-based specification of controls suitable for most organizations with a very rigorous approach to evaluation, which is suitable for high assurance requirement
Number of Control Requirement Statements	71 Static	Approximately 219 Static	2000+ based on Tailoring (360 average in scope of assessments)
Specificity of Control	Granular Requirements	Granular Requirements	Granular Requirements
Flexibility of Control Selection	No Tailoring	No Tailoring	Tailoring
Evaluation Approach	1x3: Control Implementation	1x5: Control Implementation	3×5 or 5×5: Control Maturity assessment against either 3 or 5 maturity levels
Targeted Coverage*	NISTIR 7621: *Small Business Information Security Fundamentals*	**NIST 800-171, HIPAA Security, GLBA Safeguards, DOL EBSA Cybersecurity Program, NAIC Data Security Law, NIST I7621 and Health Industry Cybersecurity Practices (HICP)**	NIST SP 800-53, HIPAA, FedRAMP, NIST CSF, AICPA TSC, PCI DSS, GDPR, and 37 others
Level of Assurance**	Low	Moderate	High
Relative Level of Effort	0.5	1.0	5.0
Certifiable Assessment	No	Yes, 1 Year	Yes, 2 Year
Complementary Assessments	None	Readiness	Readiness, Interim, Bridge
Leverages Results Distribution System (RDS) to Share Results	Yes	Yes	Yes
Leverages the AI Engine to Prevent Omissions, Errors, or Deceit	Yes	Yes	Yes

HITRUST Assessment attributes

Higher quality and reliability at every level of assurance



bC Features:

- Low level of effort and assurance
- Self-assessment only; verified by HITRUST Assurance Intelligence Engine
- 71 HITRUST CSF requirements
- 1 maturity level (Implemented)
- Provide coverage against **NISTIR 7621**, *Small Business Information Security: The Fundamentals*

i1 Features:

- Moderate level of effort and assurance
- 219 HITRUST CSF requirements (static / fixed)
- Provides strong coverage of **NIST 800-171**, the **GDPR Safeguards Rule,** much of the **HIPAA Security Rule,** and portions of **AICPA TSC**
- 1 maturity level (Implemented)
- **1-year certification**
- Uses an external assessor's annual evaluation of control implementation along with HITRUST review and QA
- Readiness Assessment available

r2 Features:

- High level of effort and assurance
- Varies from 198 – 2000 requirements, based on inherent **risk factors** and included **authoritative sources** (optional)
- Scores: Policies, Procedures, Implemented, Measured, and Managed
- Full 5x5 PRISMA evaluation using a comprehensive scoring rubric
- Able to demonstrate regulatory compliance against authoritative sources such as HIPAA and the NIST Cybersecurity Framework
- Can be bridged by a HITRUST CSF Bridge Certificate
- Readiness Assessment available
- **2-year certification**

© 2021 HITRUST Alliance

Disclosure

The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought.

Baker Tilly US, LLP trading as Baker Tilly is a member of the global network of Baker Tilly International Ltd., the members of which are separate and independent legal entities.

© 2022 Baker Tilly US, LLP.