HITRUST Demystified:

What it means and what to expect from certification

Baker Tilly refers to Baker Tilly Virchow Krause, LLP,
an independently owned and managed member of Baker Tilly International.

Today’s agenda

01 HITRUST CSF structure, applicability and benefits

02 HITRUST certification lifecycle & key milestones

03 HITRUST reporting options

04 Getting started

© Baker Tilly Virchow Krause, LLP. All rights reserved. Confidential and proprietary information.

HITRUST Alliance

HITRUST
Health Information Trust Alliance

- Founded in 2008, became non-profit in 2011
- Governed by an Executive Council comprised founders and leaders from across the healthcare industry
- Maintains the Common Security Framework (CSF)
- Educates and certifies a community of practitioners/assessors
- Provides clarification and interpretation of CSF to practitioners, assessors and clients
- Provide validated reports for all types of assessments
- Certification Authority

© Baker Tilly Virchow Krause, LLP. All rights reserved. Confidential and proprietary information.
BAKER TILLY

HITRUST Alliance

HITRUST
Health Information Trust Alliance

Mission: Establish a holistic approach for the healthcare industry to manage information security risks

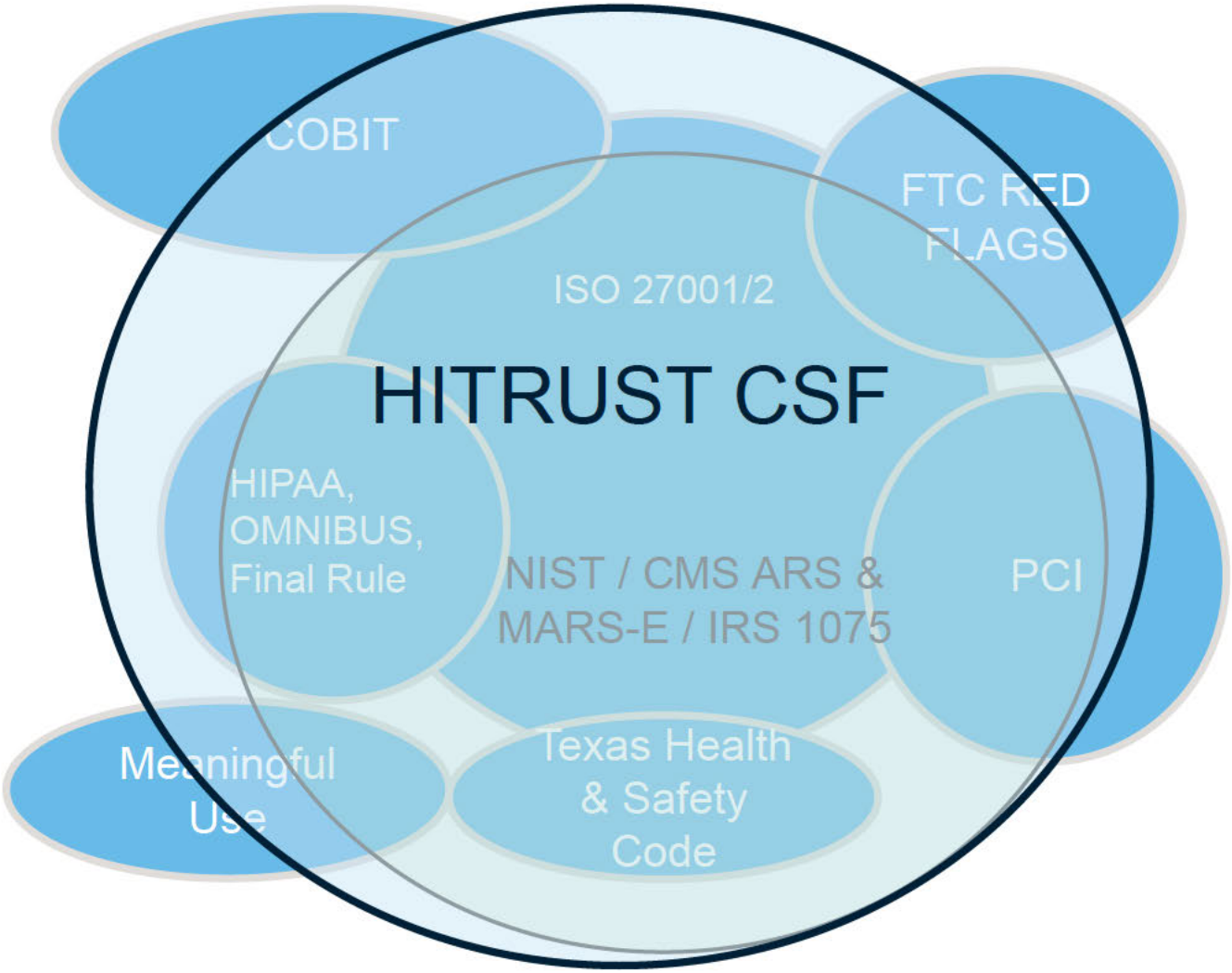
- Regulations and standards combined and aligned into a single overarching framework tailored for healthcare
- Prescriptive, scalable, certifiable
- Eliminate inconsistent approaches to certification and risk management
- Eliminate ambiguity
- Ability to cost-effectively monitor compliance of organizational, business partner and government requirements
- Provide support and enable sharing of ideas, feedback, experiences amongst the healthcare industry

© Baker Tilly Virchow Krause, LLP. All rights reserved. Confidential and proprietary information.
BAKER TILLY

HITRUST CSF Framework

The HITRUST Alliance created a Common Security Framework (CSF) to address the data privacy, security, and regulatory challenges faced by healthcare organizations, health insurance providers and other third parties that handle PHI

HITRUST CSF relationship to other standards



© Baker Tilly Virchow Krause, LLP. All rights reserved. Confidential and proprietary information.

BAKER TILLY

HITRUST benefits

- Measure compliance and identify gaps with the HIPAA Security Rule and other regulatory requirements
- Proactively identify and mitigate security risks that could influence organization's image (reputation risk) avoid penalties and possible litigation
- Preserve the trust of patients, insurers, donors, bankers, public, employees, and other key stakeholders
- Independent "second set of eyes"
- Means to assess business associates compliance with HIPAA

© Baker Tilly Virchow Krause, LLP. All rights reserved. Confidential and proprietary information.

HITRUST applicability

HITRUST
Health Information Trust Alliance

Covered Entities

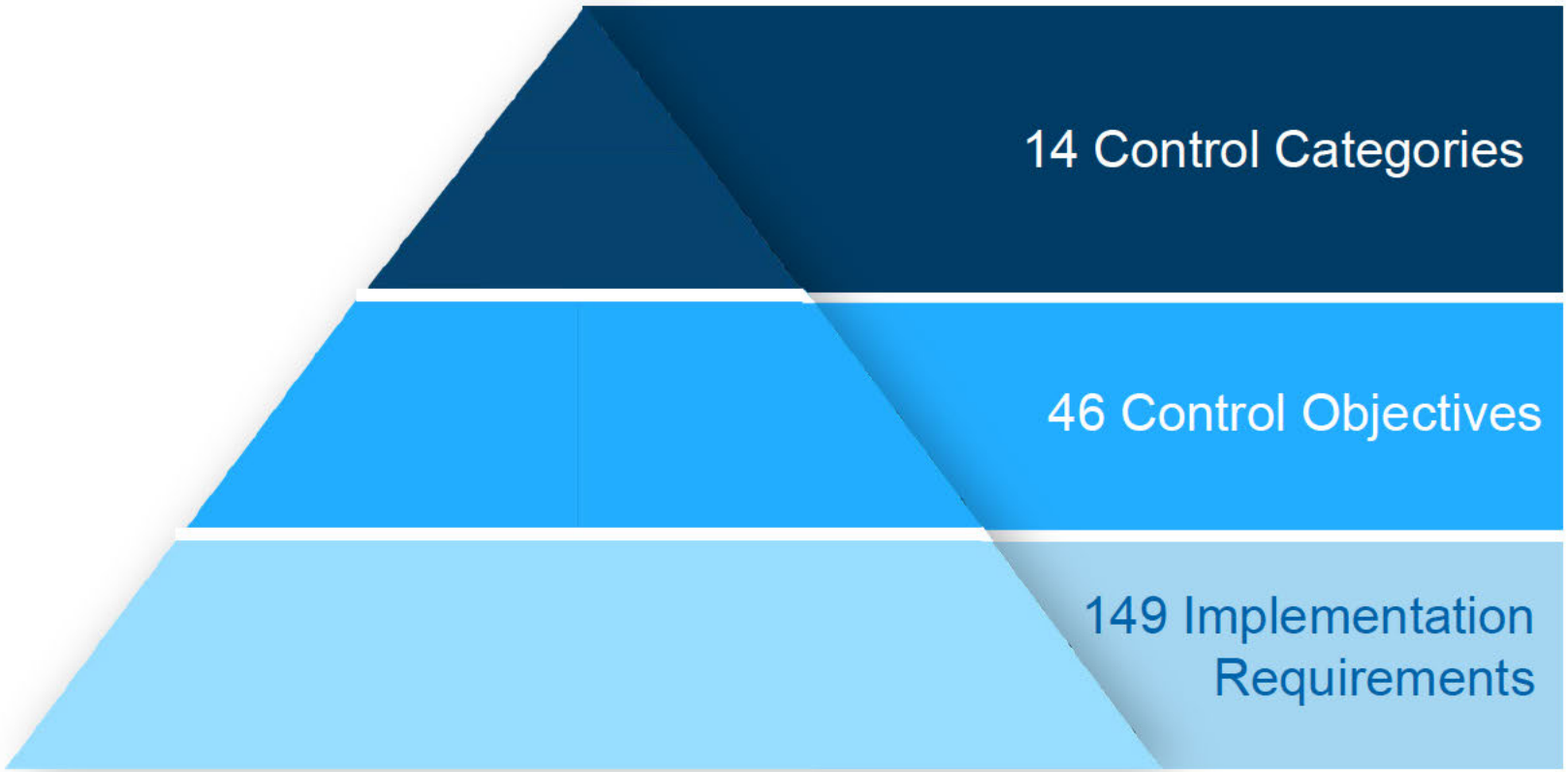
Health plans, health care clearinghouses, and healthcare providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards

Business Associate

A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity

© Baker Tilly Virchow Krause, LLP. All rights reserved. Confidential and proprietary information.
BAKER TILLY

Control Categories, Objectives and Reference



© Baker Tilly Virchow Krause, LLP. All rights reserved. Confidential and proprietary information.

HITRUST CSF
Design Detail

Categories (# of objectives and requirements in parentheses) are:

0.0 Information Security Management Program (1,1)

01.0 Access Control (7,25)

02.0 Human Resources Security (4,9)

03.0 Risk Management (1,4)

04.0 Security Policy (1,2)

05.0 Organization of Information Security (2,11)

06.0 Compliance (3,10)

07.0 Asset Management (2,5)

08.0 Physical and Environmental Security (2,13)

09.0 Communications and Operations Management

10.0 Information Systems Acquisition, Development and Maintenance (6,13)

11.0 Information Security Incident Management (2,5)

12.0 Business Continuity Management (1,5)

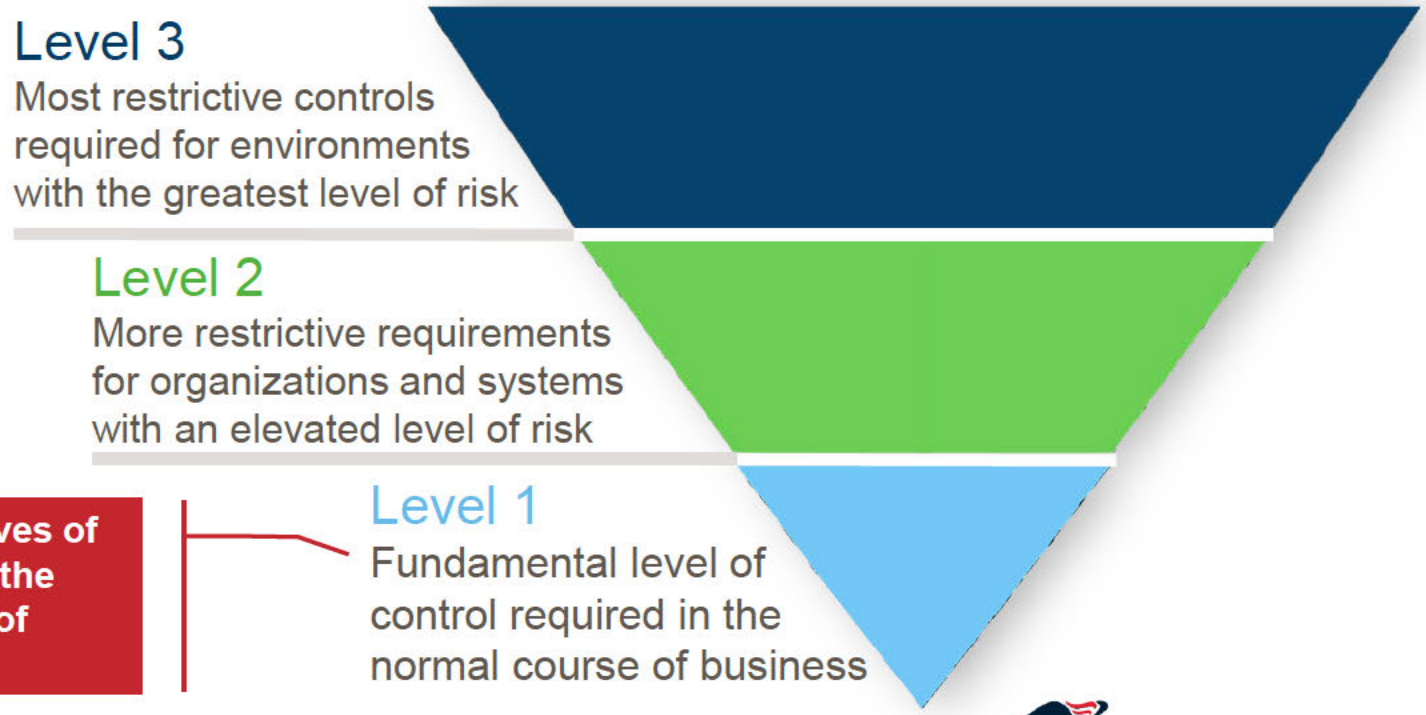
13.0 Privacy Practices (4,14)

© Baker Tilly Virchow Krause, LLP. All rights reserved. Confidential and proprietary information.

HITRUST > Scalability

Three levels of requirements are based on:

- **Organizational Factors** – defined by size and complexity of organization (i.e., number of covered lives, licensed beds, visits per year, number of employees, etc.)
- **System Factors** – defined by system attributes (i.e., stores, processes or transmits PHI, Accessibility from Internet, by third party or public, etc.)
- **Regulatory Factors** – defined by regulatory requirements (i.e., HITECH, Red Flags, JCAHO, FISMA, PCI)



Meeting the objectives of HIPAA serves as the minimum level of requirements

© Baker Tilly Virchow Krause, LLP. All rights reserved. Confidential and proprietary information.

BAKER TILLY

HITRUST Assessment Domains

1. Information Protection Program
2. Endpoint Protection
3. Portable Media Security
4. Mobile Device Security
5. Wireless Security
6. Configuration Management
7. Vulnerability Management
8. Network Protection
9. Transmission Protection
10. Password Management
11. Access Control
12. Audit Logging & Monitoring
13. Education Training & Awareness
14. Third Party Assurance
15. Incident Management
16. Business Continuity & Disaster Recovery
17. Risk management
18. Physical & Environmental Security
19. Data Protection & Privacy

- CSF library is the database of implementation requirements
- Requirements for each control are rolled up into a number of unique questions, the questions are mapped to various domains
- Scoring is done by domain

© Baker Tilly Virchow Krause, LLP. All rights reserved. Confidential and proprietary information.

HITRUST Scoring

The organization will enter responses for each requirement statement that will assess the level of compliance for each of five PRISMA-based maturity levels, which are:

1. Is a **policy** or standard in place?
2. Is there a **process** or procedure to support the policy?
3. Has it been **implemented**?
4. Is it being **measured** and tested by management to ensure it is operating?
5. Are the measured results being **managed** to ensure corrective actions are taken as needed?

© Baker Tilly Virchow Krause, LLP. All rights reserved. Confidential and proprietary information.

HITRUST Scoring

For each maturity level, the organization indicates its level of compliance with five options:

1	2	3	4	5
Non compliant (0%)	Somewhat compliant (25%)	Partially compliant (50%)	Mostly compliant (75%)	Fully compliant (100%)

© Baker Tilly Virchow Krause, LLP. All rights reserved. Confidential and proprietary information.

BAKER TILLY

HITRUST Assessment Types

CSF Security Assessment	CSF Security & Privacy Assessment	CSF Comprehensive Security Assessment	CSF Comprehensive Security & Privacy Assessment	NIST Cybersecurity Assessment
Questionnaire created utilizing ONLY the Required CSF Controls for Certification (120-328 possible requirement statements)	Questionnaire created utilizing the Required CSF Controls for Certification as well as the Privacy Controls (202-468 possible requirement statements)	Questionnaire created utilizing ALL the CSF Security Controls (271-706 possible requirement statements)	Questionnaire created utilizing ALL CSF Controls (353-846 possible requirement statements)	Questionnaire created utilizing only the most significant HITRUST CSF Required Statements that pertain to the NIST Cybersecurity Framework (120-328 possible requirement statements)

© Baker Tilly Virchow Krause, LLP. All rights reserved. Confidential and proprietary information.

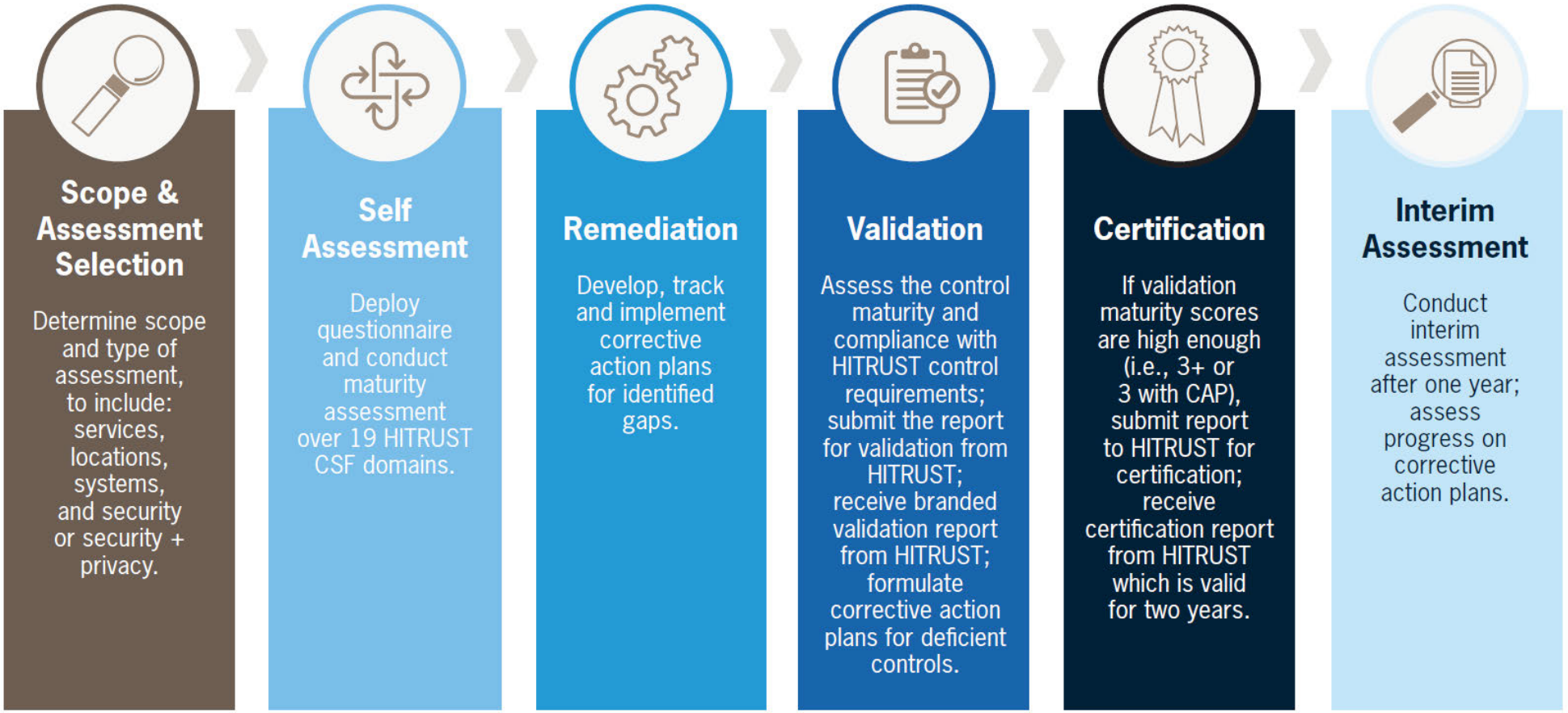
HITRUST Security Assessment

What is the Security Assessment?

- Set of questions derived from the MyCSF library spread out among 19 assessment domains
- Supports self assessment and third-party validated assessment
- Can be used as your initial compliance assessment – measure your current status
- Used to show an adequate level of security to third parties
- Designed to measure you against 66 implementation requirements (required for CSF Certification) within the CSF – not all 149
  - Provides minimum set of requirements covering each of the HIPAA Security Rule's standards and implementation specifications
  - Directly supports an entity's assertion of compliance with the HIPAA Security Rule

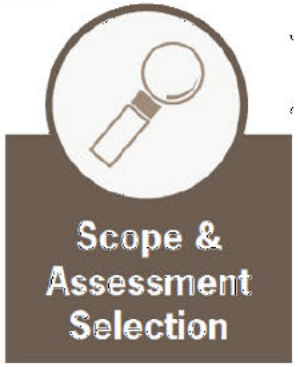
© Baker Tilly Virchow Krause, LLP. All rights reserved. Confidential and proprietary information.
BAKER TILLY

HITRUST Lifecycle



© Baker Tilly Virchow Krause, LLP. All rights reserved. Confidential and proprietary information.

HITRUST Lifecycle



Scope Carefully and Creatively

Service providers are not obligated to scope all business elements or all parts of the CSF

1 Service Offerings

Consider specific customers and prospects and overall cost-benefit of additional coverage of ePHI-related services

2 Assessment Objects

Understand the use and flow of ePHI to identify: locations, business units, services, applications and infrastructure

3 Object Grouping

Determine if the in-scope objects should be packaged as one assessment or segmented into multiple, more granular ones based on control centralization and maturity

© Baker Tilly Virchow Krause, LLP. All rights reserved. Confidential and proprietary information.

BAKER TILLY

HITRUST Lifecycle

Select Your Assessment Accurately

- Service providers are not obligated to scope all business elements or all parts of the CSF. Consider if:
  - Certification is not required by customers … yet
  - Certification required, but readiness level unknown
- Can be facilitated by a third party

	Security Only	Security + Privacy
Baseline	Focuses only on the controls required for CSF certification (120-328)*	Adds Privacy controls to the security baseline (201-468)*
Comprehensive	Includes all controls within the CSF except Privacy controls (276-705)*	Adds Privacy controls to the comprehensive security scope (387-845)*

NIST Cyber Security Assessment – Includes only the most significant controls that pertain to the NIST Cyber Security Framework (185)*

** Number of implementation requirements depends on risk factors*

© Baker Tilly Virchow Krause, LLP. All rights reserved. Confidential and proprietary information.
BAKER TILLY

HITRUST Lifecycle

Remediate

Certification requirements

- Each domain MUST score at least a 3 for a certified report
- Any implementation requirement below a 3+ will raise a Corrective Action Plan (CAP)
- Certification with a CAP is possible, but overall domain score needs to be 3
- If domains are below 3, only a validated report will be generated

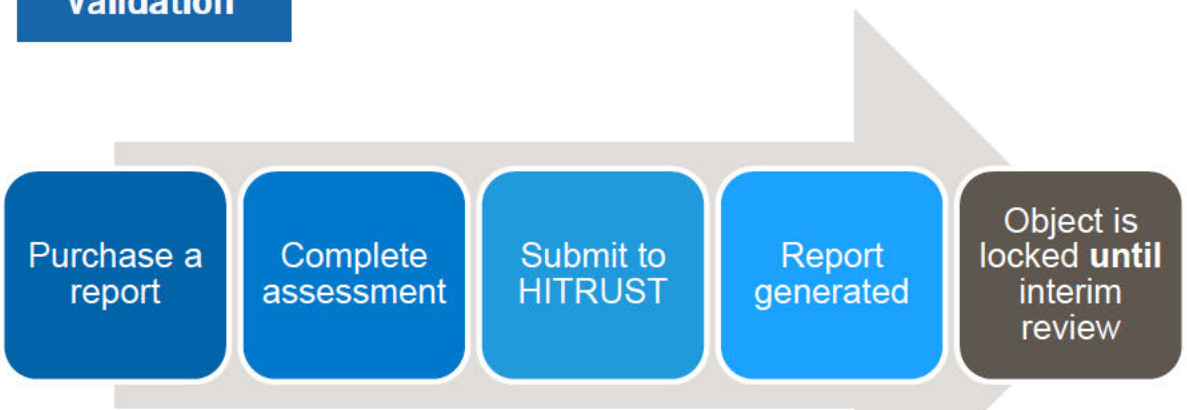
© Baker Tilly Virchow Krause, LLP. All rights reserved. Confidential and proprietary information.

HITRUST Lifecycle

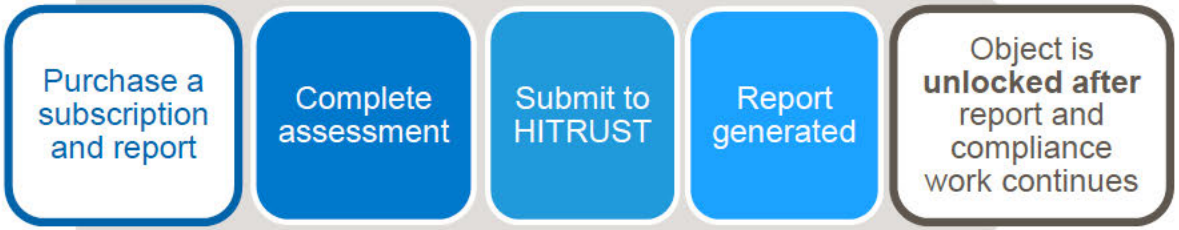
Validation

High Level Process for Validated Report

Report-only option comes with 90 days access to complete assessment. Then 30 days access is provided to response to CAPS and review report.



Report Only
**not recommended by HITRUST*



Subscription and Report

© Baker Tilly Virchow Krause, LLP. All rights reserved. Confidential and proprietary information.

BAKER TILLY

HITRUST Lifecycle

Certification

- If validation maturity scores are high enough (i.e., 3+ or 3 with CAP), submit report to HITRUST for certification.
- You will receive the certification report from HITRUST which is valid for two years.

© Baker Tilly Virchow Krause, LLP. All rights reserved. Confidential and proprietary information.
BAKER TILLY

HITRUST Lifecycle

Only applies to Certified Assessment Reports

Process – Performed at the one-year anniversary

- Update scoping questions
- Test at least 1 control/statement in each domain
- Review status of any CAPS
- Document results in a memo for HITRUST

No data security breach reportable to a federal or state agency of law or regulation occurred (e.g., Health Information Technology for Economic and Clinical Health Act (HITECH)) due to a breakdown in the service provider's control environment (Note: A reportable breach must be reported to HITRUST, who will investigate the nature of the breach to determine if de-certification is required)

**** HITRUST can remove certification if they determine progress is not being made***

© Baker Tilly Virchow Krause, LLP. All rights reserved. Confidential and proprietary information.

HITRUST
Reporting Options

HITRUST
Authorized CSF Assessor

HITRUST Validated Assessment

- Standalone assessment
- Performed by a HITRUST CSF assessor firm
- Intent of obtaining certification

SOC 2 + HITRUST Dual Opinion

- Common scope of testing
- Combined deliverable which must be delivered by a HITRUST CSF Assessor that is also a CPA firm

SOC 2 + HITRUST Validated Assessment

- Common scope of testing
- Dual opinion with the intent of obtaining certification
- Must be delivered by a HITRUST CSF Assessor that is also a CPA firm

© Baker Tilly Virchow Krause, LLP. All rights reserved. Confidential and proprietary information.

BAKER TILLY

HITRUST >
Getting started

BAKER TILLY

Getting started

Subscribe to MyCSF

- License type
- Anticipated assessment objects
- Add-ons
- Modules

Engage a CSF Assessor

- Select an assessor that fits your culture
- Industry expertise is as important as technical expertise

Scope assessment objects

- Group like objects
  - Are systems managed consistently?
- Consistent governance structure
- Centralized security policies and control systems

Define reporting requirements

- Security only assessment
- Security + privacy assessment
- Comprehensive security assessment
- Comprehensive security & privacy assessment
- NIST cybersecurity assessment

Complete self assessment

- Recovery Planning
- Improvements
- Communications

© Baker Tilly Virchow Krause, LLP. All rights reserved. Confidential and proprietary information.

BAKER TILLY

Connect with us

bakertilly.com/cybersecurity

BAKER TILLY

Baker Tilly refers to Baker Tilly Virchow Krause, LLP,
an independently owned and managed member of Baker Tilly International.