HITRUST guide

LBMC INFORMATION SECURITY

make a good business better

table of contents

INTRODUCTION 3

CHAPTER 1: WHAT IS HITRUST? 4

CHAPTER 2: THE BENEFITS OF USING HITRUST................6

CHAPTER 3: THE CHALLENGES OF DEPLOYING THE HITRUST CSF 10

CHAPTER 4: THE HITRUST ASSURANCE PROGRAM – HOW IT WORKS...11

CONCLUSION 18

ABOUT...19

introduction

If you are a healthcare organization, or a service provider that handles electronic protected health information, you know the critical importance of maintaining patient privacy and complying with HIPAA.

With the wave of highly publicized cyberattacks on healthcare, the IT challenges of data security and compliance have only multiplied. Fortunately, the HITRUST CSF can assist in meeting those challenges, and it is rapidly gaining acceptance in the healthcare security ecosystem. In this guide, we'll explore what HITRUST is, the benefits of deploying it, and how organizations can clear the high bar it can present in implementation.

CHAPTER 1:
what is HITRUST?

HITRUST is actually 3 things:

- An organization formed to advance the state of information security in the healthcare industry
- An industry-recognized security framework that can be adopted by any organization
- An Assurance Program that uses a proprietary assessment methodology for self-assessments or third party validated assessments to determine how well an organization is using the HITRUST CSF

HITRUST ORIGINS

In 2007, representatives of the healthcare industry came together to form HITRUST, with the goal of ensuring that information security would be a pillar of the industry. The HITRUST Board, with representatives from healthcare providers, insurers and vendors, understood that information security was necessary for the broad adoption of technologies that are important to patient care.

The following year, work began on a common security framework, or HITRUST CSF, to incorporate best standards in information security with the specialized needs of the healthcare industry.

HITRUST also developed a CSF Assurance Program to provide a standard way to evaluate and score information security controls either through self-assessment or by an outside assessor organization, and to set the bar for outside assessors on healthcare and information security expertise. Through the HITRUST Assurance Program, organizations can become HITRUST CSF certified.

CHAPTER 1: WHAT IS HITRUST?

WHAT THE HITRUST CSF IS, AND ISN'T

Built specifically for healthcare organizations -- and relevant third parties -- the HITRUST CSF provides a standardized guide for organizations to assess their information security risks, take corrective action, document the process, and maintain best practices. The HITRUST CSF also allows organizations to tailor the program to an organization's size or areas of specialization, while still providing an adequate level of protection.

HITRUST offers HITRUST CSF certification to organizations through its Assurance Program, although it's important to note that no regulatory bodies require HITRUST certification. However, the U.S. Department of Health and Human Services and the Office of Civil Rights consider mitigating factors such as an organization's use of a certification process, like HITRUST, in the event of a security breach. When it comes to state or other compliance issues surrounding electronic protected health information, HITRUST CSF certification incorporates many of these requirements and thereby fulfills an organization's regulatory obligations. Certification also conveys to business associates that a recognized system of IT security controls tailored to the healthcare industry is in place.

CHAPTER 2:
the benefits of using HITRUST

HIPAA (the Health Insurance Portability and Accountability Act) is perhaps one of the best known acronyms in healthcare, in part due to the ubiquitous "Notice of Privacy Practices" forms given to patients at doctor visits. But when it comes to information security requirements for operators in the healthcare space (covered entities) and the companies they work with (business associates), HIPAA is notoriously -- and intentionally -- vague in terms of providing specific, prescriptive guidance to organizations seeking to comply. This lack of specifics was meant to provide flexibility given the large variety of types and sizes of entities that deal with electronic protected health information (ePHI).

But since HIPAA was passed in the mid-1990s, the unintended consequences of its vagueness surrounding security requirements have caused an information vacuum -- it's like giving an archer a target without any real bullseye. That has led to an immature IT security environment in many parts of the healthcare industry precisely at a time when identity theft, medical fraud and other cybercrimes have skyrocketed.

The HITRUST CSF and the HITRUST CSF Assurance Program address the problems created by this vagueness by providing a standardized, prescriptive guide for healthcare organizations, with the flexibility to customize for the unique circumstances of each entity.

CHAPTER 2: THE BENEFITS OF USING HITRUST

HITRUST has a mechanism for keeping up with the rapidly changing cybersecurity landscape. HITRUST has a cyber threat working group that, in collaboration with the HITRUST Cybersecurity Threat Intelligence and Incident Coordination Center, maintains a threat catalog tied to the HITRUST CSF controls. By identifying the controls intended to address a particular threat, organizations can more easily consume threat intelligence and proactively address active and emerging threats. HITRUST issues additional guidance to organizations regarding the HITRUST CSF controls or any additional requirements when needed.

HITRUST BENEFITS FOR PROVIDERS

To illustrate the benefits of the HITRUST CSF to healthcare providers who contract for services from third-parties that need access to protected patient information to do their jobs, let's consider a hypothetical, but common, scenario.

Let's say you are a medium-sized regional health system, and you have established a security program to the best of your ability using the required and addressable safeguards outlined in the HIPAA Security Rule.

You likely have a compliance officer and in-house counsel who provide some oversight to make sure you are doing your best to meet the baseline regulatory requirements. Security is by no means perfect or completely impenetrable, but you get the picture -- you are for the most part "normal."

CHAPTER 2: THE BENEFITS OF USING HITRUST

Like most healthcare organizations, you rely on a bevy of third parties to assist you in your mission to provide care for your communities. Just to name a few, you contract with several billing/collection companies for different claim types, have agreements with contract physician groups, medical transcription services, reference labs, technology support providers, financial audit firms, as well as many others. The list of organizations that work with the protected health information of your patients certainly isn't endless, but it's pretty long.

Some of those organizations are covered entities in their own right; others are purely business associates who, for one reason or another, need to access your patient data. There are contracts in place with all of these organizations, but you know in your heart of hearts that some do a much better job with securing data than others. You also know that while they will ultimately be liable from a contractual and regulatory standpoint for any breach they cause, your organization is still on the hook as the upstream covered entity, and will face significant reputational harm if your organization's name ends up on the HIPAA "Web Wall of Shame" for data breaches exceeding 500 records, even if it was the fault of one of your business associates.

The HITRUST program offers you the opportunity to reduce heartburn over potential breaches, both by deploying it in your own health system and requiring HITRUST CSF certification from these third parties.

HITRUST BENEFITS FOR BUSINESS ASSOCIATES

Let's flip things around in this next hypothetical scenario for a different perspective.

CHAPTER 2: THE BENEFITS OF USING HITRUST

Let’s say you are a company that prepares billing statements for hospitals -- in other words, you are one of those business associates mentioned in the previous example. Fortunately for your business, you have hundreds of customers just like the health system we previously described. Some are smaller, some larger, but all have concerns about how well you are protecting their ePHI.

Security requirements formerly glossed over in their contracts and business associate agreements are now expanding as they adopt more formal vendor management programs. About half of those clients want you to either provide some type of independent audit report or answer their questionnaire about information security.

Since there isn’t a government-approved HIPAA certification report, and you haven’t engaged with a firm to perform another security-focused audit like a SOC 2, and because your customers don’t have a single audit reporting format, you are left with filling out their security questionnaires. Unfortunately, that leaves you with dozens of questionnaires to fill out. Each asks some of the same questions, but usually in different ways. Some are 50 questions; some are 300 or more. It’s beginning to feel like you spend more time responding to customer questionnaires than you do maintaining the security of your systems.

Obtaining certification under the HITRUST CSF has the potential not only to reassure you about the strength of your information security, but also to provide you with credentials that are accepted by many healthcare providers without the need to muck through the questionnaire swamp.

CHAPTER 3:
the challenges of deploying the HITRUST CSF

There is no way around it — deploying the HITRUST CSF and being reviewed under the Assurance Program is complex and time-consuming.

The HITRUST CSF is prescriptive – in some cases, very prescriptive. If you are just using HITRUST CSF as a good framework, you can certainly pick and choose what works best within your organization to adequately address your security risks. But if you are looking to be certified against the HITRUST CSF (see Chapter 4), you will need to be prepared to make some tweaks to your existing policies, procedures, and control activities.

How major those tweaks are will depend on the maturity of your security program and the framework upon which it is built. Our experience tells us that even organizations that have obtained certifications around ISO or PCI are often surprised that there is still some heavy lifting to do as they dig into the requirements of the HITRUST CSF.

Third Party Management is a great example of where the prescriptive requirements of the HITRUST CSF often out-pace the current practices of many organizations. The implementation guidance related to some of the required controls in this domain go to the level of describing language that should be included in contracts and agreements with third party vendors, and often require enhancements to both existing policies and those legal documents.

CHAPTER 4:

the HITRUST assurance program – how it works

Since many organizations who adopt HITRUST will want to communicate their compliance with the HITRUST CSF to various internal and external stakeholders, HITRUST developed their HITRUST Assurance Program. Self-Assessment reports are available from HITRUST for organizations that do not have a need to provide independent assurance of their compliance. For others whose customers require a higher level of assurance, validated reports are used. Validated assessments are performed by independent assessor organizations that have been vetted and approved by HITRUST. A validated report can also be a “certified” report if the target organization achieves a minimum level maturity score in each of the domains in the HITRUST CSF.

HITRUST CSF assessments, whether they be a self-assessment or a validated assessment performed by a third party, utilize HITRUST’s portal application called HITRUST MyCSF™. HITRUST My CSF™ is built on top of a Governance, Risk, and Compliance software platform that serves as a multi-purpose portal, giving the organization access to the entire CSF library as well as the option to create different types of assessments.

To access the My HITRUST CSF™ portal, the organization must pay HITRUST a fee for either a subscription or for a one-time assessment. To create an assessment, the organization will identify the in-scope business units, locations, and systems along with a number of organizational, system, geographic, and regulatory factors. Based on that input (particularly system and regulatory factors), the My HITRUST CSF™ tool builds a customized assessment.

Rather than provide the control requirement as published in the framework, a series of baseline security statements are generated. They break down the broader requirements of the HITRUST CSF into more manageable chunks. To put this in concrete terms, while there are roughly 66 HITRUST CSF controls required for certification, an organization could easily have 250 to 300 (or more) baseline statements generated as part of their assessment.

It probably goes without saying, but to do this right takes time. HITRUST provides very prescriptive guidance on how to properly score each category using illustrative procedures that serve as a "floor" for guiding how an assessor will evaluate your compliance. If you are being assessed for the first time, be aware of consultants who claim they can "get you certified" in a few weeks. It's just not possible. Even without all the work that goes into scoring, HITRUST's own review period after your assessment is turned in for adjudication, and report issuance is 4-6 weeks.

Formal HITRUST CSF certification can take six months to a year to complete, and multiple years for larger organizations. Once certification is complete, it lasts for two years, with a less intense assessment occurring in year two.

ASSESSMENT IS NOT PASS/FAIL

One common misconception about becoming HITRUST CSF certified is that it is a binary, pass/fail endeavor. Rather, each baseline statement is evaluated on a 1 to 5 scale that equates to a percentage of compliance in five maturity categories. Those categories are Policy, Process, Implemented, Measured, and Managed.

EVALUATING REQUIREMENTS STATEMENTS

The following table provides a minimum generic set of criteria (questions) based on the general requirements for full compliance, which assessors should consider when evaluating a requirements statement at each level of the model, as they provide the necessary context for scoring against the specific evaluation criteria contained in HITRUST's illustrative procedures, which are discussed at more length in the next section.

LEVEL	GENERIC EVALUATION CRITERIA
1 – Policy	• Do formal, up-to-date policies or standards exist that contain "shall" or "will" statements for each element of the requirement statement? • Do the policies and standards that exist for each element of the requirement statement cover all major facilities and operations for the organizations and/or systems/assets in scope for the assessment? • Are the policies and standards that exist for each element of the requirement statement approved by management and communicated to the workforce?
2 – Procedures	• Do formal, up-to-date, documented procedures exist for the implementation of each element of the requirement statement? • Do the procedures clarify where the procedure is to be performed, how the procedure is to be performed, when the procedure is to be performed, who is to perform the procedure, and on what the procedure is to be performed? • Do the procedures address each element of the requirement statement across all applicable facilities, operations and/or systems/assets in scope? • Are procedures for the implementation of each element of the requirements statement communicated to the individuals who are required to follow them?
3 – Implemented	• Is each element of the requirements statement implemented in a consistent manner everywhere that the policy and procedure applies? • Are ad hoc approaches that tend to be applied on an individual or on a case-by-case basis discouraged?
4 – Measured	• Are self-assessments, audits and/or tests routinely performed and/or metrics collected to evaluate the adequacy and effectiveness of the implementation of each element of the requirements statement? • Are evaluation requirements, including requirements regarding the type and frequency of self-assessments, audits, tests, and/or metrics collection documented, approved and effectively implemented? • Does the frequency and rigor with which each element of the requirements statement is evaluated depend on the risks that will be posed if the implementation is not operating effectively?
5 – Managed	• Are effective corrective actions taken to address identified weaknesses in the elements of the requirements statement, including those identified as a result of potential or actual information security incidents or through information security alerts? • Do decisions around corrective actions consider cost, risk and mission impact? • Are threats impacting the requirements periodically re-evaluated and the requirements adapted as needed?

Table 2. Generic Evaluation Criteria by Maturity Level

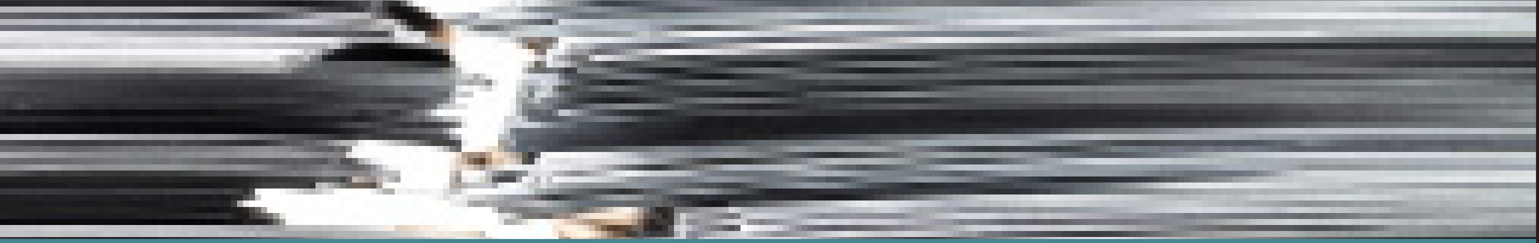
HITRUST's scoring methodology can be a little daunting for both the initiated and uninitiated alike. To achieve certification without any noted corrective action plans, the organization must score a "3+" on the PRISMA scale (a maturity model-based scoring system) in each of the 19 domains that make up the HITRUST CSF. An organization can still be certified with a PRISMA score of 3 in one or more domains, but corrective action plans will be included in the report for those domains falling below a 3+. If any domains score below a 3, the organization can receive a validated report, but cannot be certified.

Scoring is performed at the baseline security statement level for each of the categories (Policy, Process, Implemented, Measured, Managed). The scores at this level are done as percentages as follows:

1 = 0% (non-compliant)
2 = 25% (somewhat compliant)
3 = 50% (partially compliant)
4 = 75% (mostly compliant)
5 = 100% (fully compliant)

One key to understanding (or not mis-understanding) scoring is that the 1-5 scale listed above does not correlate to the PRISMA score. PRISMA scores are derived from the computed percentages using a weighted average. The weighting for the control categories is as follows:

- Policy – 25%
- Process – 25%
- Implemented – 25%
- Measured – 15%
- Managed – 10%



The calculation of the weighted average of all of the control statements required for certification within a domain are then mapped to the PRISMA scale. As a reference point, a PRISMA score of 3+ is achieved at a weighted average of greater than 70.99.

As a practical matter, the weighting that HITRUST has placed on the first 3 maturity categories means your most rapid path to certification is achieving high scores (preferably 5 / 100%) for Policy, Process, and Implemented. With scores of 5 in each of these categories, even if Measured and Managed score 0, the weighted average would be 75%, placing the organization above the certification threshold.

At a high level, the HITRUST validated assessment involves:

- Assessors gathering and examining documentation (e.g., policies, procedures, records, logs, vulnerability assessment reports, risk assessment reports)
- An examination of configuration settings, physical surroundings, processes and other observable information protection practices
- Conducting interviews with business unit stakeholders, where applicable
- Performing system tests to validate the implementation of controls, as applicable
- Updating the assessor portion of the client's HITRUST MyCSF™ assessment instance with the appropriate scoring information and assessment documents.

CONSIDER CAREFULLY THE SCOPE OF YOUR ASSESSMENT

With all the rigor involved with an assessment, defining its scope is of critical importance. Obviously if your certification report will be shared with third parties, the scope of your assessment needs to be relevant to the systems those business associates care about.

CHAPTER 4: THE HITRUST ASSURANCE PROGRAM – HOW IT WORKS

While many of the policy and procedure requirements of the HITRUST CSF would be considered organizational or entity level controls, a large number are directly tied to systems (in this context, “system” refers to a collection of information systems components that serve a particular business purpose). The more systems that are in-scope, the more testing will be required. Even though sampling techniques will be used by your assessor, those samples will need to include selections from each in-scope system. Keeping that list restricted to only the systems needed for the assessment will save you time and money.

Avoid the temptation (as nice as it sounds) to come out of the gate with an “enterprise” certification assessment unless it is absolutely necessary. Be sure to work with an assessor organization that has experience in working with companies on a collaborative basis to get them over the HITRUST goal line.

DO YOU NEED A VALIDATED THIRD PARTY ASSESSMENT?

A self-assessment is going to be a requirement for any organization looking for a validated or validated / certified assessment using a third party assessor. However, it often becomes apparent that even the self-assessment process can be overwhelming for organizations that don’t already have a robust IT security program in place due to the number of controls and the amount of documentation required to accurately provide scoring against the framework.

The HITRUST CSF was designed to be customizable for an organization’s unique set of needs. That too can be a challenge for internal teams that may not have the requisite knowledge to scope and score their internal assessment. We recommend that organizations consider sending one or more internal stakeholders to HITRUST training before embarking on the assessment process. Even with, but especially without, training, a company should consider engaging an approved assessor organization to guide them through scoping decisions that may have a huge impact on the work effort involved in the assessment.

The primary reasons for engaging an assessor for a validated assessment are 1) the benefit of an independent, objective set of eyes, 2) contractual mandates from customers to obtain a validated or certified report, or 3) the value of having a validated report in terms of competitive advantage or at least equivalence when working with prospective customers.

HITRUST has a rigorous selection process for designating approved assessors. Assessors must demonstrate expertise in both healthcare and information security, have sufficient resources to carry out assessments, document their assessment processes and quality controls, and participate in initial HITRUST training and continuing education.

conclusion

Securing electronic protected health information is a major challenge for healthcare organizations and their business associates, but deploying the HITRUST CSF offers a prescriptive path that makes that challenge surmountable.

Obtaining HITRUST CSF certification is a complex undertaking, but the rewards can be large, enabling organizations to address regulatory requirements and business challenges. Most importantly, HITRUST assists them in meeting a fundamental responsibility – to honor the trust that patients place in them every day to safeguard some of the most private information about their lives.

LBMC information security

While regulatory compliance is mandatory, so is operating a successful business. A well-designed information security program provides critical intelligence about risks facing your business so your executive team can make well-informed decisions.

As a member of the family of LBMC companies, LBMC Information Security separates itself from traditional information security firms by offering practical, cost-effective solutions that are customized to your unique risk environment. We tailor our assessments and deliverables to your organization's risk tolerance, providing the highest level of risk reduction for the associated cost. These practical solutions lead to real results and a tangible return on investment.

HITRUST SERVICES

One of a select group of HITRUST CSF assessors, LBMC Information Security participated in the effort to integrate security standards from Centers for Medicare and Medicaid Services and NIST into the HITRUST framework. Based on this deep security and compliance expertise, we are exceptionally well qualified to use the HITRUST CSF to assure healthcare entities, their patients and government regulators that protected health information is safe and secure.

LBMC INFORMATION SECURITY

make a good business better