TEVORA™

Case Study

Tevora Helps Small Health Information Exchange Leverage HITRUST™ to Punch Above its Weight

If your organization handles Protected Health Information (PHI), you probably know that safeguarding this data is critical to your success. Achieving HITRUST™ certification is a great way to ensure that your sensitive information is secure while letting your customers know that you take data security and privacy seriously. It can also be the key to unlocking new markets and opportunities. For example, HITRUST™ certification can help healthcare vendors open the door to new contracts with large health insurance providers.

In this case study, we'll describe how Tevora helped a small Health Information Exchange leverage HITRUST™ certification to compete with larger competitors to win business in a new state. To protect our client's confidentiality, we'll refer to them by the fictitious name of Health Exchange Solutions (HES) and will not divulge the state in which they won the new business.

What is HITRUST™?

Before we dive into the HES case, let's explain what HITRUST™ is.

The HITRUST™ organization provides a framework that safeguards PHI and helps manage information risk for organizations across all industries. Since its inception, HITRUST™ has become widely regarded as the benchmark for information security compliance in the healthcare industry.

The HITRUST™ Common Security Framework (CSF) addresses a multitude of security, privacy, and regulatory challenges facing healthcare organizations today. With a comprehensive framework of security requirements, HITRUST™ incorporates a risk-based approach to federal and state regulations and common standards and frameworks to help organizations address these challenges.

There are 19 Domains covered in HITRUST™ certification (e.g., Information Protection Program, Endpoint Protection, Portable Media Security). Each Domain has multiple requirements that are individually scored. The total number of requirements for an assessment are calculated based on various factors such as organization type, size, and location. To achieve compliance, an organization must receive a composite score of at least 62% across all requirements for a given Domain.

Until recently, organizations wishing to obtain HITRUST™ certification were required to undergo a rigorous HITRUST™ Common Security Framework (CSF) Validated Assessment performed by a third-party External Assessor organization that has been approved by HITRUST™ to perform these assessments.

In January 2023, HITRUST™ announced two new assessment options to accommodate organizations with different levels of risk exposure. With these additions, HITRUST™ now offers three assessment alternatives:

- **The Essentials, 1-Year e1 Validated Assessment (New).** The HITRUST e1 Assessment is designed to cover basic Foundational Cybersecurity practices that address the assurance needs of lower-risk organizations. The e1 requires less effort to complete.
- **The Implemented, 1-Year (i1) Validated Assessment (New).** Suitable for moderate-risk scenarios or where a baseline risk assessment is needed. HITRUST™ Authorized External Assessors will validate i1 Validated Assessments.
- **Risk-Based, 2-Year(r2) Validated Assessment (Current).** This is the new name for the CSF Validated Assessment. Otherwise, the requirements are the same. Suitable for higher-risk scenarios. HITRUST™ Authorized External Assessors will validate r2 Validated Assessments.

As a HITRUST™ Authorized External Assessor, Tevora is fully qualified to perform e1, i1 and r2 Validated Assessments. Our team of experienced healthcare security experts can also help you bring your organization into compliance with HITRUST™ requirements to ensure you are ready for a Validated Assessment.

Now that we've provided some background on HITRUST™, let's move on to the HES case.

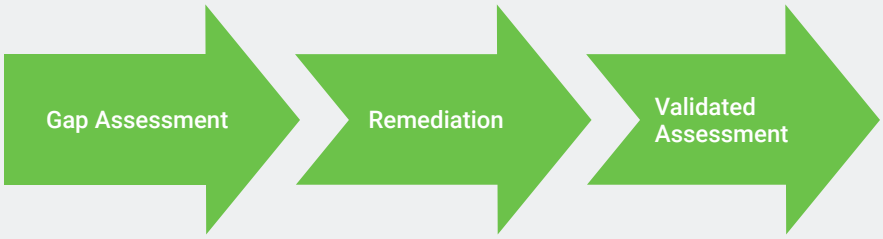
Tevora Engaged

In 2017, HES was presented with an opportunity to significantly expand its business into a new state, but it needed HITRUST™ CSF certification to pursue the expansion. As a small organization with only two employees responsible for security and infrastructure, they knew they would need outside help to compete with larger organizations to win this business. After evaluating several leading cybersecurity consulting firms, HES engaged Tevora to help them achieve HITRUST™ CSF certification.

Kickoff Meeting

Our first order of business was to hold a kickoff meeting to meet key staff members and learn about GSS's objectives, business operations, and overall security and technical environment. We also reviewed our methodology for helping clients achieve HITRUST™ CSF certification. Here's a summary of the methodology:

Tevora's Proven HITRUST™ Methodology



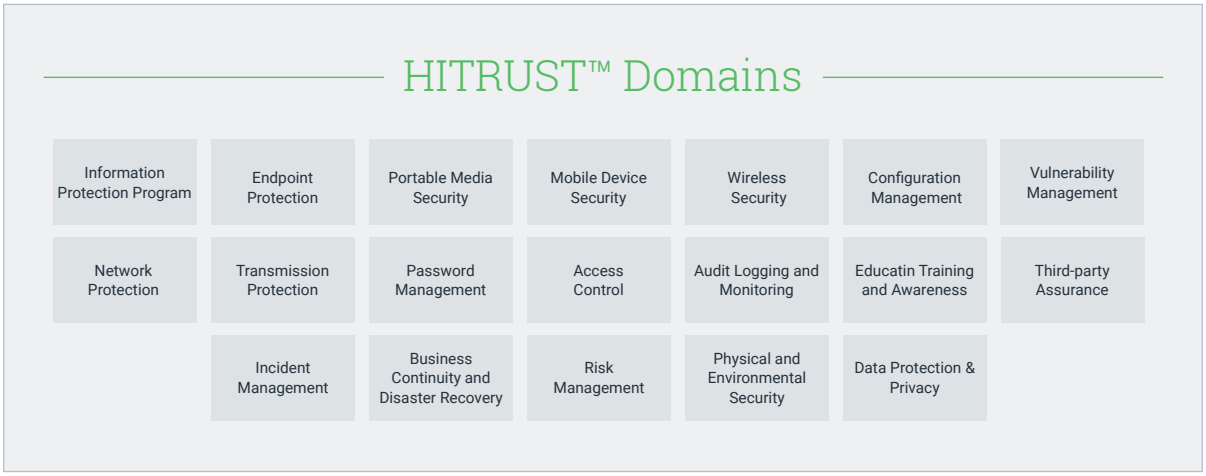
- Identify gap areas where client environment falls short of HITRUST™ requirements
- Outline cost-effective, focused strategy for addressing gaps

- Work with client to make changes needed to achieve HITRUST™ certification (e.g. writing security policies, implementing security controls
- Help client use MyCSF™ portal to perform self-assesment

- Validate that HITRUST™ controls are in place based on scope and applicable controls defined during self-assessment
- Provide validation scores for each key control Domain to determine if certification criteria are met

We explained that it generally takes 10-12 months to transition from the gap assessment to the point where HITRUST™ issues certification for most clients. We highlighted that our experienced team of security consultants could dive in and complete most of the remediation work, or if HES preferred to do the work, we could serve more as an advisor during this phase. With its limited security staff, HES elected to have Tevora perform a majority of the remediation work.

We also provided HES with a high-level review of the 19 Domains included in the HITRUST™ framework (see below) and explained that to achieve compliance, they would need to receive a composite score of at least 62% for each Domain.



Project Planning

After the kickoff meeting, we met individually with key HES stakeholders to map out a plan for achieving HITRUST™ CSF certification. The plan detailed tasks to be performed by HES and Tevora staff with target dates for each. We assigned an experienced project manager to shepherd the plan through to successful completion.

Initial HITRUST™ CSF Certification

Once the plan was reviewed and approved by HES management, we launched the project to help HES achieve HITRUST™ CSF certification for the first time.

After performing a gap assessment to identify areas where HES fell short of HITRUST™ requirements, we made remediation recommendations. We worked side-by-side with their team to design and implement feasible and realistic controls to address the identified gaps. This work included activities such as writing or modifying policies and procedures and implementing technical solutions to enhance security and privacy.

We used a highly collaborative, iterative approach to test the new controls for each Domain as they were implemented. When testing revealed that a control failed to meet Domain requirements, we jumped in to help HES shore up the control, then re-tested it, repeating the process until we reached a composite score of 62 percent or more for each Domain.

After providing the final Domain scores to HES, we helped them request and obtain formal HITRUST™ certification from the HITRUST™ organization.

The successful certification was achieved in August 2018, on time and within budget. HES management was thrilled with the results. Their HITRUST™ certification enabled them to fend off larger competitors to win the business for operating in the new state, a major accomplishment for their small organization.

Building On Success

To maintain HITRUST™ CSF certification status, HITRUST™ requires organizations to perform full assessments every other year and reduced-scope interim assessments during the years in-between. Based on their positive experience with the first HITRUST™ assessment, HES engaged Tevora to conduct these assessments on an ongoing basis, and they continue to be a valued customer today. Over the years, our partnership has deepened, and we are frequently called on to provide cybersecurity advice and services in addition to our HITRUST™ work.

Overcoming Challenges

Helping HES successfully maintain their HITRUST™ certification status and meet state-specific security requirements over the years has not always been easy. We've had to go the extra mile to help them successfully overcome many significant challenges along the way.

Addition of MARS-E

In 2020, the Department of Health in the state where HES expanded its operations raised the security bar by requiring compliance with Minimum Acceptable Risk Standards for Exchanges (MARS-E) controls in addition to the HITRUST™ requirements. This increased the total number of controls that HES needed to comply with from the roughly 650 required for their 2018 HITRUST™ certification to well over 800.

When we learned of the new MARS-E requirement, we had a relatively short timeframe to react. Because HES still had a small number of security resources, they asked us to ramp up our team to respond to the MARS-E requirement in the same timeframe as, and coincident with, the originally-planned effort for HITRUST™ 2020 certification. We responded by immediately assigning additional Tevora security experts to help develop new controls and enhance existing ones—and develop new policies, procedures, and documentation—to address the MARS-E requirements. By quickly adding these resources and putting in some long days, our team was able to help HES successfully certify for both HITRUST™ and MARS-E on time and within budget in 2020.

Adapting to COVID-19

Another significant challenge for HES's 2020 certification was reacting to the business practice changes necessitated by the COVID-19 pandemic. When it became clear that COVID-19 was going to drastically change the way in which businesses operate, we worked with HES management to quickly revise our certification plans to incorporate remote work wherever possible. For example, our revised plans called for all walkthroughs to be performed virtually. We also agreed to strictly adhere to social distancing and mask guidelines to minimize infection risk when there were no alternatives to on-site work. With careful planning, close partnership with HES, and significant dedicated and focused work, we met our schedule and budget targets for 2020 certification.

Working with State Department of Health

Tevora took a lead role in interfacing with the Department of Health in the state where HES had expanded its operations. This included representing HES in monthly and quarterly Department of Health meetings to report on certification progress, understand and adapt to new state-level security and privacy requirements, and ensure that HES was meeting the state's requirements for funding support of HES's operations. This required Tevora to draw on its deep well of experience working with state agencies to address the Department of Health's concerns, questions, requirements, regulations, and bureaucratic hurdles, which were myriad.

> Tevora has developed a strong working relationship with HES and built a reputation as their go-to player

State Raises the Security Bar Again

The state Department of Health raised the bar for security again in 2022 by adding regulations that require compliance with a new security framework. This brought the total number of controls HES had to comply with to over 900. Again, Tevora was called on to enhance security and privacy controls and make other needed changes to meet the new requirements. We have allocated additional resources and are currently working with HES to modify controls, policies, and procedures to address the new regulations. At this point, we're on track for a November 2022 certification.

Benefits of Using Tevora's HITRUST™ Compliance Services

As outlined in this case study, Tevora has developed a strong working relationship with HES and built a reputation as their go-to player for a broad range of cybersecurity services. We believe this mutually successful relationship was enabled by the unique benefits that Tevora brings to the table, including:

- **Expertise and Experience.** Tevora's in-depth healthcare and security knowledge and proven compliance methodologies smooth your path to compliance.
- **Insightful Advice.** We take the time to get to know your people and learn about your organization's unique pressures and challenges. This enables us to provide insightful advice that is tailored to your environment.
- **Approved HITRUST™ Assessor.** As an approved HITRUST™ Authorized External Assessor, we are fully qualified to perform the recently-announced i1 and r2 Validated Assessments.

Our sweet spot is at the intersection of healthcare security expertise and deep client relationships. Whether it be providing strategic insights or rolling up our sleeves to help implement security solutions, we pride ourselves in doing whatever it takes to ensure our clients are successful.

Let us be your trusted partner

If you'd like to learn more about how Tevora can be your trusted security partner, just give us a call at **833.292.1609** or email us at **sales@tevora.com**.