HITRUST

CASE STUDY

To Ensure Vendor Security: UPMC Turns to the HITRUST CSF Assessment to Help Manage Third-Party Risk

John Houston, VP, Privacy and Information Security & Associate Counsel, UPMC

Overview

UPMC is partnering with an ever-increasing number of vendors—many of which are moving their applications and data services to the cloud. As a result, UPMC found that it was ineffective to individually assess the information security and compliance of each of its vendors. UPMC solved this problem by utilizing the HITRUST CSF and related assurance program. By requiring vendors to become HITRUST CSF certified, UPMC can more effectively manage information risk and trust the security and compliance levels of third-party vendors and know that all organizational and patient data will remain protected.

The Challenge: Move to the Cloud Escalates the Need for Data Security Assurance

UPMC is a $19 billion world-renowned health care provider and insurer based in Pittsburgh. With a focus on inventing new models of accountable, cost-effective, patient-centered care, the organization employs 85,000 people—including 4,800 physicians—and operates 40 academic, community and specialty hospitals as well as 600 doctor offices and outpatient sites.

UPMC LIFE CHANGING MEDICINE

UPMC needed an effective method for assessing the information security and compliance levels of its third-party vendors that had access to ePHI or other sensitive information. The organization solved this problem by utilizing the HITRUST CSF framework to assess the security and compliance levels of these vendors. The prescriptive controls found in the HITRUST CSF also creates a common language for conversations about a vendor's security and compliance gaps that need to be addressed—a benefit that can prove useful at all levels within the organization and across the vendor ecosystem.

Headquarters: Pittsburgh, PA
Number of Employees: 85,000
Industry: Healthcare

UPMC's move to cloud-based services sharply escalated the need for a third-party security and compliance risk management program. "In the past, we could more easily secure information because it was only stored in our on-premises data center," says John Houston, Vice President of information security at UPMC. "Today, that same data is not always in our possession, so we have to rely on cloud platform providers and third-party vendors to properly secure our most sensitive information."

As processing patient information in the cloud became more prevalent, UPMC needed to set up a program to ensure that data no longer in its physical possession was still secured appropriately—according to both internal policies that UPMC established and the industry regulations and standards that the organization must follow, such as HIPAA.

"In addition to assessing current vendors and getting them to agree to be HITRUST CSF Certified for security and compliance, we needed to evaluate new vendors," Houston says. "Our main focus initially was to make certification a requirement for entry into our vendor environment."

For business associates, UPMC is making HITRUST CSF certification for security and compliance part of the contract and a requirement to conduct business. In some cases, UPMC will penalize vendors if they do not become certified by a specified date.

"Over time, we plan to work with existing vendors for HITRUST CSF certification as contracts come up for renewal and as we expand the services we utilize with each vendor," says Houston.

The Solution: HITRUST Provides Flexible Security Control Framework for Assessing Vendors

To take on the challenge of assessing third parties for their security and compliance maturity, UPMC turned to a long time partner that the organization has trusted for many years.

"We have used the HITRUST CSF since 2009 as our own security framework, and currently, we are using an external assessor to perform a HITRUST CSF assessment," says Houston. "It helps us make sure all of our IT systems are secure and in compliance with all the major regulations and standards."

The HITRUST CSF enables organizations of any size—from small supplier businesses to large organizations—to address the challenge of complying with the multitude of federal, state and industry regulations, standards and frameworks pertaining to information security—both on-premises and in the cloud. By incorporating a risk-based approach, the HITRUST CSF provides a comprehensive and flexible framework of security controls:

- Harmonizes and cross-references globally-recognized standards, regulations and business requirements—including ISO, NIST, PCI, HIPAA and state laws.
- Scales controls according to organizational type, size and complexity.
- Provides prescriptive requirements to ensure clarity.
- Offers multiple implementation requirement levels as determined by specific risk thresholds.
- Allows for alternate control adoption when necessary.
- Evolves according to user input as well as changing industry and regulatory conditions.

In addition to UPMC using the HITRUST CSF to guide internal security and compliance assessments, independent external auditors that work with the organization also rely on the framework.

"That shows you how well-respected HITRUST is by our industry," says Houston. "We've been committed to HITRUST for a long time and find great value in using the framework to make sure our IT systems protect the sensitive information of the organization and our patients."

The Results: Framework Facilitates Discussions on Vendor Security and Compliance Gaps

With the move of UPMC services to the cloud and the reliance on third parties who manage UPMC data in the cloud, the HITRUST CSF was the natural vehicle for UPMC to rely on in order to make sure business associates apply the appropriate controls to keep information secure.

"We decided to utilize the HITRUST CSF because HITRUST has historically focused on healthcare and rolls up all the relevant standards and regulations into a single framework that's cohesive to work with," Houston says. "We can look at one framework and be assured it covers all of the regulations and standards pertaining to our industry with which we have to comply."

Utilizing the HITRUST CSF also comes in handy when an external organization asks about UPMC compliance with a particular regulation or standard. "An organization

HITRUST CSF Solution Highlights

- Enables UPMC to trust the security and compliance levels of third-party business associates and know that all organizational and patient data will remain protected.
- Provides a common framework that makes it easy to compare each vendor to industry norms.
- Creates a common language for conversations about vendor security gaps that need to be closed.
- Eliminates the need for internal UPMC auditors to assess vendor security and compliance maturity.
- Serves the UPMC vendor community by giving them a certification they can share with other healthcare providers rather than having to respond to separate security questionnaires.

recently asked if we comply with NIST," Houston says. "Because NIST is built into the HITRUST CSF, we could say 'yes' right away and with confidence. We could even provide a certification score to prove our level of maturity around the NIST cybersecurity framework; that's a feature that most other common frameworks do not provide."

Houston also appreciates that the HITRUST CSF creates a common language around security and compliance that UPMC and its vendors can use to have conversations on any risks that need to be addressed. "Most of our vendors already know what the HITRUST CSF is," says Houston. "It's a widely-accepted standard with a certification process, so when vendors show us their certification, we can understand exactly what it means."

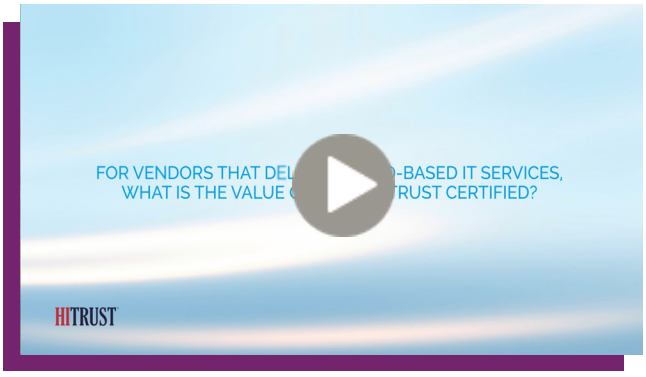
Houston compares the HITRUST CSF to a nationwide chain of retail stores or restaurants: "You know that the products or food and the services of a chain store will be the same no matter which place you go into," he says. "With HITRUST certification, you can be certain that the report you get from one vendor will align to what you get from another vendor. That makes it easy to confirm their certification score and understand any gaps they might have."

A One-Stop-Shop for Vendor Assessments

Because each vendor has gone through the same process to get certified, Houston can easily interpret what the gaps mean and the level of security and compliance maturity an organization has achieved.

"When comparing internal audits, such as SOC 2, it's not nearly as easy as comparing one HITRUST assessment to another," says Houston.

For those vendors who do not know what the HITRUST CSF is, Houston says that when he explains it, the framework immediately makes sense, and the vendors understand what UPMC is trying to achieve. The framework has become a one-stop-shop that UPMC can go to for all-around certification of its third-party business partners.



This streamlines the process, eliminates confusion, reduces supply chain risk, and ultimately increases the security posture of the entire healthcare ecosystem. This, in turn, increases the ability for all involved in delivering patient care to do just that: deliver patient care.