HITRUST

CASE STUDY: CHANGE HEALTHCARE LEVERAGES HITRUST MYCSF

Change Healthcare Leverages HITRUST MyCSF to Maintain ISO 27001 Certification

Security control assessment reports mapping quickly to ISO 27001 requirements to help avoid audit nonconformity while also reducing the amount of time spent by the internal InfoSec team

About Change Healthcare

Change Healthcare (NASDAQ: CHNG) is a leading healthcare technology company focused on insights, innovation, and accelerating the transformation of the US healthcare system. The company provides data and analytics-driven solutions to improve clinical, financial, administrative, and patient-engagement outcomes.

The Challenge: Enable Acquired Business Unit to Maintain ISO Certification

Change Healthcare processes approximately 20% of all healthcare transactions in the US—about 15 billion every year. With services and systems spanning the processing of insurance claims, payments for medical services, and prescription payments, Change Healthcare connects insurance companies and care providers to help drive improved patient care.

As Change Healthcare acquired a McKesson business unit specializing in cardiac imaging, radiology, and CT scan systems, the InfoSec team faced a unique challenge. The business unit had established customer business associate agreements (BAAs) that required maintaining ISO 27001 certification for the systems within the scope of this offering. When it was time for another audit, the ISO auditor wanted a view into Change Healthcare's security posture—not just any view; they wanted a view specifically focused only on the area contained within the scope of the acquired business unit.

Fortunately, the risk management program at the company-wide level was already mature. That's because Susan Richards, Director of Information Security, began an effort in 2015 to help the company achieve certification with the HITRUST CSF framework. Susan's team had done a thorough job mapping controls to compliance requirements. This work would prove extremely valuable, even if the driver behind this work was different.

CHANGE HEALTHCARE

This HITRUST case study presents how Change Healthcare leveraged the HITRUST CSF® and the HITRUST MyCSF® portal to enable one of its business units to maintain ISO 27001 certification. The certification was necessary for a process providing technical support on medical imaging systems. The MyCSF portal provided access to HITRUST CSF reports documenting the security controls of the system, and these reports presented the ISO auditor with the required risk register views to pass the audit. Without the MyCSF reports, the Change Healthcare InfoSec team would otherwise have to spend an exorbitant amount of time providing the necessary risk views. The organization may have also received a nonconformity score that would have required security control mitigations that business unit customers would have been aware of. But with the HITRUST MyCSF, Change Healthcare found they already had a helpful tool that made it possible to quickly present the security posture of any system.

Headquarters: Nashville, TN
Number of Employees: 15,000
Industry: Healthcare Technology

© 2022 HITRUST

"We went through a risk assessment of the business unit during the acquisition using the HITRUST MyCSF tool," says Richards, speaking to the compliance readiness view she was looking to garner from the tool. "We typically look at HITRUST as a compliance management framework, but for the ISO audit, we realized it's also a risk management framework," she adds, noting the risk assessment activities as they relate to validating compliance against several regulatory requirements.

For the ISO audit, the challenge was two-fold:1) present the results only for the business unit in scope, and 2) change the internal InfoSec team's mindset from compliance assessment activity to a risk management audit. There are also differences between the ISO process and the HITRUST process. ISO involves an audit, whereas the HITRUST Approach includes an assessment and a review by HITRUST with validation by an independent third party.

"An ISO audit is less collaborative," Richards says. "The auditor asks if you have a control in place and if you can prove it. If you can't, they don't advise on how to prove it. We were more accustomed to the HITRUST Approach where assessors advise on how to close security control gaps."

The Solution: HITRUST CSF Assessment Reports Map to ISO Requirements

The imaging business unit hosts system information on the Google Cloud Platform. The assessment of the security controls for this environment was included in the HITRUST certification that Change Healthcare had previously achieved. For the ISO 27001 certification, the auditor was specifically looking at how Change Healthcare handled technical support for customer systems without compromising the integrity of private health information. Customer contracts require the Change Healthcare support process to be ISO 27001 certified, so customers know the process is secure.

The auditor spent a lot of time on the ISO risk management clauses during the ISO assessment, looking at how the imaging business unit approaches risk management. This included evaluating how risks are assessed, where the risk register is stored, how risk is mitigated, and who in the organization owns each risk.

Because the assessment data already existed and was immediately available via their MyCSF portal, Change Healthcare could leverage its previous HITRUST efforts to pull the required report for the auditor, explicitly scoped to the areas for which the auditor was concerned. Change Healthcare needed to scope the business unit's security posture, map it to the controls required for ISO 27001, and produce the report that the auditor wanted.

> "We showed the ISO auditor how our HITRUST risk assessment reports attested to our level of control implementations," Richards says. "We also produced a report that matches what the auditor was looking for in a risk register. We leveraged the HITRUST MyCSF as a risk management framework for achieving ISO certification by enabling him to see everything in one place. This shows how MyCSF serves as a tool that lets us easily switch between compliance certifications (such as HIPAA) and audit assessments (such as ISO)."

HITRUST CSF Highlights

- Protects PHI, PII, and digital assets from cyber-criminals.
- Proves attestation to regulations pertaining to sensitive information and digital assets.
- Generates one report that demonstrates to all customers that their data is secure.
- Reduces the cost and time spent by IT on compliance audits requested by customers.
- Provides a framework to measure the security and compliance postures of partners.
- Raises the level of awareness of security and compliance importance across the company.

HITRUST MyCSF Highlights

- Best-in-class software as a service information risk management platform for assessing and reporting information risk and compliance.
- Makes it easy and cost-effective for an organization to manage information risk and meet international, federal, and state regulations concerning privacy and security.
- Reduces overall assessment management costs.
- Provides continuous visibility of risk posture.
- Features are built to streamline and simplify organizational risk assessment needs.
- MyCSF Compliance and Reporting Pack for HIPAA automatically compiles evidence to save time.

© 2022 HITRUST

The Value: Avoids Potential of Nonconformity and Saves Time for InfoSec Team

With the HITRUST MyCSF portal, Change Healthcare was able to produce the information for the auditor without a huge delay and without much effort beyond what they already put into MyCSF for the overall company. Change Healthcare can also use this same model next year and the year after—keeping it consistent for internal security assessments and certifications and other activities performed by external auditors, such as for ISO 27001.

"For each risk category, we were able to point to a MyCSF report that shows the control level," says Richards. "The auditor viewed the reports as the same risk register view he was used to seeing. Every ISO 27001 risk management clause maps to a HITRUST control, which allowed us to demonstrate the security of the customer support process."

Richards also points out control perfection is not absolutely necessary to achieve ISO 27001 certification. "If there are gaps, the auditor mainly wants to see that you have assigned someone to mitigate the gaps. In that sense, the HITRUST CSF reports serve as an internal guide to help us plan how to improve our security posture. As we go through the HITRUST assessments, their independent assessors provide us with feedback on how to close the gaps identified—that's a big differentiator from the approach of ISO auditors. HITRUST is prescriptive as far as advising us on the solution for closing any security gaps we have."

The HITRUST assessment consolidated all the risk assessment information into a format the ISO auditor wanted to see, complete with the gap information managed via HITRUST's Corrective Action Plan (CAP) module. By having this information at-the-ready in HITRUST MyCSF, Richards was able to demonstrate the current status of the program specific to the scope required by the auditor while avoiding time-consuming activities and conversations of persuasion. " It would also have required much more time from my team because we would need to identify one person to take responsibility for that risk information and keep a separate risk register up to date."

The Future: Micro Security Control Analysis Enables and Protects Business Growth

Looking ahead, Richards says, "HITRUST MyCSF is a valuable tool. If we are in a situation where a customer or auditor wants to see system security controls at a micro level, such as an API, MyCSF enables us to do this with very little work. We can target assessments to a particular product or system."

By leveraging the HITRUST CSF framework and the MyCSF portal, Change Healthcare processes transactions more efficiently. And with better information and better decision making, that drives better service for the business units and partners, which then ultimately drives better care for patients.

"If you're using HITRUST strictly as a risk management framework, look at it as a compliance framework," Richards recommends. "And if you're looking at it strictly as a compliance framework, see how you could use it as a risk management framework. It truly is both and helps you become a champion who enables and protects business growth."

© 2022 HITRUST