HITRUST Common Security Framework (CSF)

What to Expect During the Certification Process

Introduction

As technology plays an ever-increasing role in enterprises across every industry sector, secure data transmission and storage are becoming exponentially more critical and complex. This is further complicated by the myriad of requirements from both federal and state governments as well as third-party organizations, and an increasing threat from hackers and others with malicious intent. Ensuring adequate data security is now a critical requirement for all covered entities and their essential business associates and partners.

What is the HITRUST CSF?

In collaboration with leading privacy, information security, and risk management experts from both public and private sectors, HITRUST develops, maintains, and provides broad access to its risk and compliance management frameworks, related assessments, and assurance methodologies. The HITRUST Common Security Framework (CSF) provides organizations, and their business associates with a robust, flexible, and scalable approach to manage regulatory compliance and risk management across multiple compliance frameworks.

The HITRUST CSF provides the structure, transparency, guidance, and cross-references to authoritative sources organizations globally need to be certain of their data protection compliance. The initial development of the HITRUST CSF leveraged nationally and internationally accepted security and privacy related regulations, standards, and frameworks – including HIPAA, ISO, NIST, PCI, and COBIT – to ensure a comprehensive set of security and privacy controls, and continually updates and incorporates additional authoritative sources. The HITRUST CSF standardizes these requirements, providing enterprises with clarity and consistency and reducing the burden of compliance. The framework ensures that all security programs are aligned to efficiently support the organization's information risk management and compliance objectives.

Why Does My Organization Need to be Certified?

Originally designed for healthcare organizations, the HITRUST Common Security Framework is now leveraged by enterprises in every industry sector. By obtaining HITRUST CSF Certification, enterprises can ensure that all of their critical data is appropriately safeguarded. The certification enables organizations to confidently demonstrate to others that it has a solid, security framework in place that addresses the full range of standards and regulatory requirements. The CSF assessment results can also serve as a recognized, objective benchmark that organizations can use to manage and measure their compliance and security programs' effectiveness going forward.

TECH LOCK®
A RevSpring Company

320 E. Big Beaver Rd., Suite 145 • Troy, MI 48083
info@techlockinc.com
847.245.3727

What to Expect During the HITRUST Certification Process

Is the HITRUST CSF Certification Difficult to Obtain?

Depending on the level of security and compliance expertise within the organization, a HITRUST CSF Certification can be obtained by in-house personnel. But it can be a very time-consuming and difficult process for an already over-burdened IT and security team. By leveraging the expertise of an accredited and experienced HITRUST CSF assessor firm, the process can be very straightforward once the scope and the objectives of the project are clearly articulated, freeing up IT and security teams to focus on other critical initiatives.

What Type of Assessment is Best for My Organization?

There are two HITRUST CSF assessment options to choose from: Self assessments or validated assessments.

HITRUST CSF Self Assessment

A HITRUST self assessment is a good choice for organizations looking to minimize the effort and costs associated when demonstrating compliance with the HITRUST CSF. It can also be performed before launching a more vigorous, validated assessment. The self assessment provides an increased assurance level to the relying entity, but no official HITRUST CSF Certification is obtained. It only generates a HITRUST-issued Self Assessment Report identifying gaps in security or other procedural flaws that need to be corrected before undertaking a validated assessment.

HITRUST CSF Validated Assessment

A validated assessment is performed on-site by an authorized CSF assessor. At the completion of the audit, the assessment results are sent to security experts at the HITRUST organization for review. If all assessment criteria are met, an official HITRUST CSF Certification is issued. But if the organization fails to receive a rating of 3 or higher on any of the controls, HITRUST only provides a validated report instead of the CSF Certification, indicating where the certification levels were not met and more work is needed.

What Steps are Involved in a HITRUST CSF Assessment?

Define the Scope of the Assessment

To start the certification process, the certified HITRUST CSF assessor will meet with the client organization to define the scope and goals of the project and available resources, and then choose what type of assessment to initiate. The scoping exercise should identify all key systems, applications, facilities, and datasets that are used to create, receive, maintain, or transmit all sensitive data and information. During the scoping process, it is also essential to identify the key business and technology stakeholders who can facilitate the adoption of the HITRUST CSF within the organization.

320 E. Big Beaver Rd., Suite 145 • Troy, MI 48083
info@techlockinc.com
847.245.3727

What to Expect During the HITRUST Certification Process

Obtain Access to the HITECH MyCSF Portal

During the next step in the certification process, the firm undergoing assessment should obtain a MyCSF software subscription directly from HITRUST. After purchasing the SaaS subscription, the client will access the MyCSF portal and start uploading all key information, including the organizations existing security policies and procedures already in place.

Perform a Self Assessment

Self assessments can be performed by well-trained individuals within the assessed organization's IT or security team, however they are usually performed by an accredited HITRUST CSF assessor firm. By using an approved assessor firm, the organization can ensure they are using the most appropriate HITRUST CSF assessment methodologies, while saving considerable time and effort required when performing an in-house evaluation.

After the organization has obtained access to the MyCSF portal and uploaded the requested information, the HITRUST CSF third-party assessor will examine the flow of data between all included systems and identify any possible gaps in security protocols. This assessment should identify and rank potential gaps by risk level, providing the ability to conduct any possible remediation steps before the self assessment begins.
By conducting a self assessment before the validated assessment, organizations can reduce the risk of not achieving HITRUST CSF certification. The self assessment will determine if all security controls are properly designed prior to seeking validation, identify key stakeholders in the organization, help define a comprehensive set of remediation goals, and provide a better understanding of the HITRUST CSF processes.

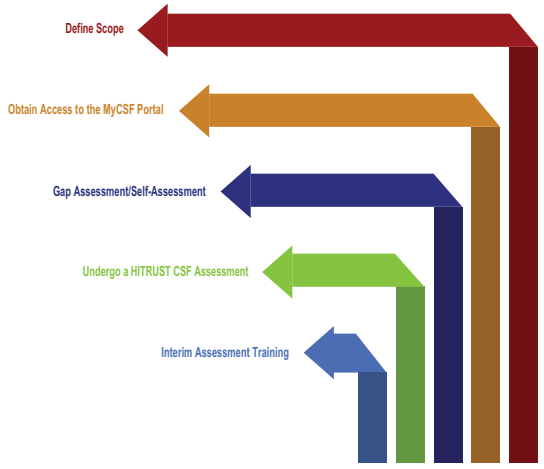
Conduct Self Assessment Remediation

After completing the self assessment, any security gaps, vulnerabilities, or other non-conformities will be identified. The organization will be able to remediate any control irregularities or deficiencies prior to launching the more comprehensive validated assessment project. This will also reduce the cost and time associated with launching into a validated assessment program from the onset.

Perform a Validated Assessment

When the self assessment is finished and all remediation activities are completed, an organization can advance to a validated assessment performed by an approved HITRUST CSF assessor firm. After the certified assessor completes the validated assessment, the assessor will submit the results directly to HITRUST for approval. Assessments that meet or exceed all HITRUST CSF scoring criteria will result in the organization receiving an official HITRUST CSF Certification. For organizations that fail to achieve a 3 or greater for each of the nineteen HITRUST CSF domains of the scoring criteria, a validated report is issued that will indicate what areas need to be addressed before a full certification can be awarded.

The HITRUST Assessment Roadmap



320 E. Big Beaver Rd., Suite 145 • Troy, MI 48083
info@techlockinc.com
847.245.3727

What to Expect During the HITRUST Certification Process

Conduct Interim Assessment Testing

The HITRUST CSF Certification is valid for two years before a full recertification process needs to be completed. At the one-year anniversary of certification, the assessed organization must conduct an interim assessment no later than sixty days after the HITRUST CSF certification anniversary date. The interim assessment must be performed by an accredited HITRUST CSF assessor firm and requires the assessor firm to test at least one requirement from each domain, test any outstanding Corrective Action Plans (CAPs), and issue an opinion letter to HITRUST. After meeting all criteria, HITRUST will then decide whether to extend the original CSF Certification for an additional year.

If HITRUST updates its specifications after the full assessment is complete, organizations are not required to align with the new standard until after their interim assessment is also finished. At the end of the two-year cycle, the next full assessment will need to align with any changes made to the certification specifications.

TECH LOCK HITRUST CSF Certification Services

TECH LOCK believes security management, threat detection, and compliance together deliver greater value when combined as a respected service. Cohesive orchestration and optimization across these disciplines provide customers with better insights into their overall security posture. TECH LOCK makes it easy to quickly adapt to the security and compliance changes that mid-size organizations and their affiliates need more than ever to protect their business. TECH LOCK is a fully accredited HITRUST CSF assessment organization, offering a range of services from self assessment and validated assessment HITRUST CSF services, managed vulnerability and remediation prioritization services, to threat detection and response.

TECH LOCK can help customers perform a HITRUST CSF self assessment with its in-depth knowledge and understanding of the requirements and unique scoring of the standard. Completing a self assessment will help customers new to the HITRUST framework understand how close they are to certification before undertaking a validated assessment.

TECH LOCK can also audit and complete a validated assessment with the customer. Validated assessments can lead to official HITRUST Certifications based on the validated assessment score. It is recommended that new clients complete a self assessment first to understand where they are at from a security standpoint. TECH LOCK can assist with every step of the assessment, with a streamlined process that will and help the firm understand all aspects of the audit.

HITRUST
CSF Certified

About TECH LOCK Inc.
TECH LOCK enables organizations to navigate, detect, and respond to today's modern cybersecurity and compliance challenges. Our full spectrum security-centric approach delivers value to our clients through defined and measurable outcomes combined with independent cyber research, specialized skills, and premium customer support and service.

320 E. Big Beaver Rd., Suite 145 • Troy, MI 48083 info@techlockinc.com 847.245.3727

TECH LOCK Inc, @ Copyright 2021