Jacobian
Engineering
An employee owned company

HITRUST Certification Process

SUMMARY

HITRUST certifies applications that run in server or cloud environments. They do not certify companies or mobile applications. The application acts as the nexus for determining scope and additional elements are brought into scope that "touch" or support the application. These generally include servers, databases, network devices (including VPNs and endpoints that use VPNs), edge devices and facilities (physical or virtual such as a cloud account).

Jacobian Engineering has been a HITRUST assessor since 2017 and has developed a process that enables customers to achieve certification in the least amount of time with the least risk and impact to the organization's resources. To do that, it is recommended to divide the project into two major phases: the readiness assessment and validated assessment.

The readiness assessment is normally quoted for a 90-day period but may be extended based on how much support an organization may need. Organizations that have not implemented a security framework such as NIST, COBIT, ISO27k or CIS, often need 2-6 months of remediation in order to develop policies, procedures and implement controls. Cloud customers, through the shared responsibility model, can often achieve parity with the minimum standards for certification under HITRUST during the 90-day readiness assessment period—others may require additional time to remediate gaps. HITRUST will not allow a control to be scored unless it has been in place **90 days prior to submitting the assessment to an assessor for validation**.

Following the readiness assessment, the validated assessment process begins and generally takes between 60 and 90 days. During this time, sampling of controls occurs to validate implementation and scoring. Documentation is reviewed and interviews are conducted. Upon completion, the assessor will submit the assessment object to HITRUST for QA validation.

Once HITRUST has received the assessment object, it goes into a queue. During Covid, the length of time to receive a draft report was as high as 12 weeks. HITRUST does not provide a service-level-agreement or estimate at any time during the process. Once the object is assigned to a QA assessor at HITRUST, the process generally completes in 2-4 weeks and a draft report is issued.

Once a draft report is issued, gaps identified during the assessment will need a correct action plan defined by the customer. Jacobian will help customers with this process and the customer will upload the CAPs to the MyCSF tool. Customers have 30 days to complete this process and ask HITRUST for any corrections to the report. After CAPs have been uploaded and the report is signed off by the customer→ CONGRATULATIONS! You will now receive your validated final HITRUST report containing your new certification!

Phase	**Purpose**	**Timing**
Readiness Assessment	• Assessment object(s) are created based on scope (or copied from self-assessment object(s)) • Customer uploads/updates all documentation and answers all the control questions. Jacobian assessors work with Customer during the Readiness assessment period to understand how to map requirement statement to their particular environment. • Setup inherited controls with providers participating in the HITRUST inheritance program (Such as AWS) • Customer submits object for validation to Jacobian assessor	90 days (this can be extended for an additional fee)
Customer remediation period	• Correct and remediate missing controls if the scoring in any domain is < 3. *(Note: All controls must be in place >90 days prior to submitting for validated assessment)* • Upload new evidence and submit.	This varies based on the readiness of the customer. Typically, SMB customers with < 100 employees where there has not been a prior assessment (such as a SOC2), implementation of a security framework such as CIS, NIST or ISO, and no prior risk assessment, this can be anywhere from 2-6 months
Validated Assessment	• Assessor collects additional evidence • Assessor validates all of the customer answers based upon the evidence provided and collected • Assessor performs on-site assessment for facilities in-scope unless 100% cloud-based or third-party	90 days

HITRUST Adjudication/QA	• Assessor submits assessment object to HITRUST • HITRUST responds within 1-2 weeks if there are any questions about major deliverables within the assessment. • HITRUST places the assessment in a queue • The assessment is assigned to HITRUST QA professional. • HITRUST works with Jacobian on any QA related questions. • HITRUST completes QA and issues validated report	In 2020, the average time to complete QA was 10-12 weeks. HITRUST does not provide an SLA or estimate.

Key factors that affect timing:

- Availability of key personnel – It is recommended that there is more than one resource, when practicable to ensure that there can be rapid turnaround for questions and information during assessment. Most SMBs should plan to spend about **1.25 resource hours per control statement** That means that an assessment object containing 350 control statements will require approximately 2.6 FTE months to complete the readiness assessment (entering data and scoring).
- Readiness for assessment – The more policies, procedures and the completeness of implementation all affect the length of time for assessments as this will reduce the time to remediate gaps needed to have a passing score.
- Availability of evidence – Documentation and access to key personnel, technical data, samples and related information are all needed by the assessor in order to complete the validation step. The more structure and process in an organization such as document management and internal wikis will all help speed the process of validation. In addition, it's imperative that documentation is updated and current. Documentation including penetration tests, policies and other supporting evidence must be less than 12 months old at the time the assessment is submitted for validation.

Some additional general information:

What is HITRUST?

The HITRUST Alliance was formed in order to promote information security as a core principle inside organizations rather than an obstacle through its Common Security Framework. CSF supports and standardize implementation of common controls that includes factors across many existing standards and regulations including HIPAA, NIST, PCI, COBIT and others.

HIPAA regulations, in particular, are comprised of a series of standards, requirements and advisories. HIPAA and the related laws and regulations are not prescriptive and, as a result, many organizations and auditors have interpreted the requirements differently. HITRUST and many in the healthcare industry believe that some of the key challenges in information security addressed by CSF are:

Inconsistent implementation of acceptable minimum controls

Inefficient w/ varying interpretation of control objectives and safeguards

Increasing scrutiny of auditors, orgs and customers

Increasing liability to organizations that are vulnerable to attack

Regulatory violations and extortion

Public concern

Inability to implement security in medical devices and applications

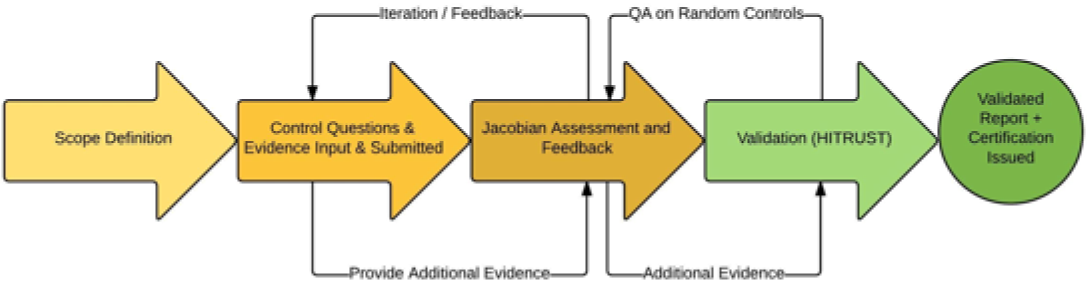
Rapidly changing business and regulation needs

The HITRUST CSF provides a consistent approach to regulatory compliance and risk management principles. The CSF is updated annually or as deemed necessary by the HITRUST council. Within the CSF, there are 156 control reference, 49 control objectives, 14 control categories, 3 implementation levels and 19 domains. The CSF provides prescriptive statements to support the establishment and maintenance of a control to meet regulatory and business goals for information security.

Jacobian Engineering's Role

Jacobian Engineering partners with organizations that wish to apply and use the Common Security Framework and achieve HITRUST certification. Jacobian employees are highly trained IT professionals, auditors, security engineers and program managers. Jacobian, as an organization, has gone through examination and review by HITRUST in order to achieve HITRUST assessor certification. Jacobian staff have become certified as HITRUST practitioners in order to help our customers understand and navigate the CSF and HITRUST process.

HITRUST Assessment Process


Iteration / Feedback
QA on Random Controls
Scope Definition
Control Questions & Evidence Input & Submitted
Jacobian Assessment and Feedback
Validation (HITRUST)
Validated Report + Certification Issued
Provide Additional Evidence
Additional Evidence

Scoping & Kickoff

Scoping is probably the most important part of the entire process. During this phase, the customer will need to ask "What and why am I doing this?". While the answer to this question may seem simple, it helps set the stage for the rest of the exercise. The Common Security Framework (CSF) is based upon ISO 27001 and includes controls from several frameworks and regulatory required standards including HIPAA, PCI, COBIT, SOC and others.

At a minimum, it is recommended that the scope include all facilities, systems, processes and personnel that process, store or transmit protected health information (PHI).

At a kickoff meeting, led by Jacobian, our auditors will work with stakeholders to define the scope and review the entire process leading up to validation and certification. If Jacobian is engaged for a readiness assessment, we will spend additional time training staff on the use of MyCSF, refining the scope and grouping like-objects to determine the minimum number of assessment objects needed for a validated assessment.

After the scope is input into the MyCSF tool, one or more assessment objects will be created. Each assessment object will have up to several hundred control questions that must be answered.

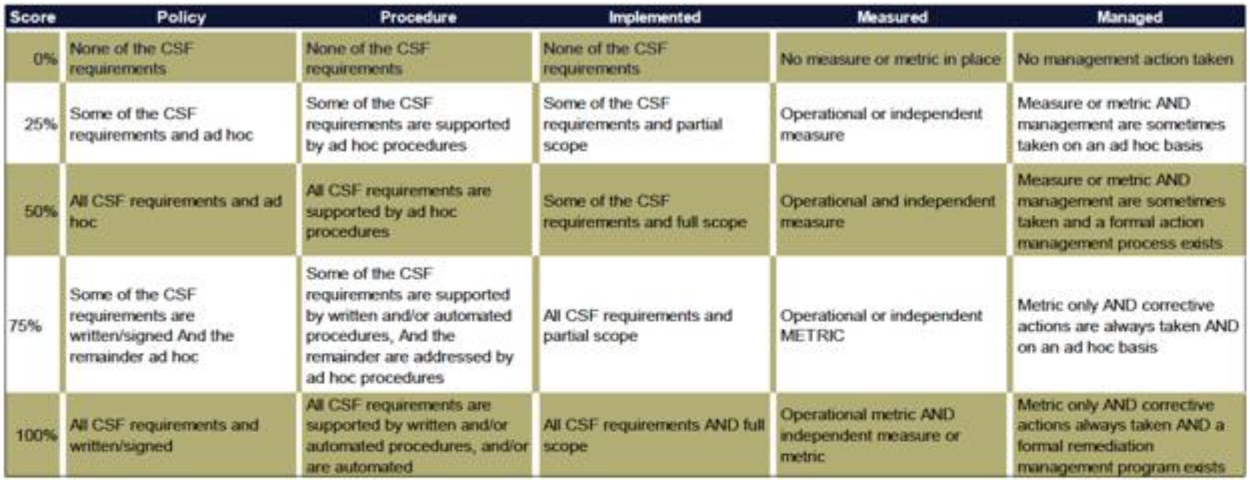
Information Gathering & Input to MyCSF

During this phase, the customer's staff will review all of the control questions for the assessment object(s) and begin answering the 5 PRISMA level questions. The PRISMA-level questions will try to answer:

Is a **policy** or standard in place?
Is there a **process** or procedure to support the policy?
Has it been **implemented**?
Is it being **measured** and tested by management to ensure it is operating?
Are the measured results being **managed** to ensure corrective actions are taken as needed?

For each maturity level, the organization will indicate its level of compliance:

Non-compliant (0%)
Somewhat compliant (25%)
Partially compliant (50%)
Mostly compliant (75%)
Fully compliant (100%)



Score	Policy	Procedure	Implemented	Measured	Managed
0%	None of the CSF requirements	None of the CSF requirements	None of the CSF requirements	No measure or metric in place	No management action taken
25%	Some of the CSF requirements and ad hoc	Some of the CSF requirements are supported by ad hoc procedures	Some of the CSF requirements and partial scope	Operational or independent measure	Measure or metric AND management are sometimes taken on an ad hoc basis
50%	All CSF requirements and ad hoc	All CSF requirements are supported by ad hoc procedures	Some of the CSF requirements and full scope	Operational and independent measure	Measure or metric AND management are sometimes taken and a formal action management process exists
75%	Some of the CSF requirements are written/signed And the remainder ad hoc	Some of the CSF requirements are supported by written and/or automated procedures, And the remainder are addressed by ad hoc procedures	All CSF requirements and partial scope	Operational or independent METRIC	Metric only AND corrective actions are always taken AND on an ad hoc basis
100%	All CSF requirements and written/signed	All CSF requirements are supported by written and/or automated procedures, and/or are automated	All CSF requirements AND full scope	Operational metric AND independent measure or metric	Metric only AND corrective actions always taken AND a formal remediation management program exists

Based on each answer, the customer will upload documentation and evidence and/or note in the comments section how it can be demonstrated to Jacobian during the on-site assessment.

Jacobian Assessment & Feedback

After all of the control questions have been answered and all supporting evidence is provided to Jacobian, the customer will submit the report to Jacobian for assessment. Jacobian will review all control answers and evidence and then schedule an on-site visit if need be, to gather additional evidence, conduct interviews, randomly sample data and test technical controls.

Jacobian may conduct direct inspection of configuration objects, penetration testing, vulnerability assessment scanning, log review and more in order to validate and test all of the answers. Once all the information is gathered, Jacobian will continue the assessment process remotely. On-site inspection is required by HITRUST for facilities included in-scope. For facilities with similar controls and processes, a "representative" facility may be inspected in lieu of visiting all facilities in order to reduce timeline and expense.

During the remainder of the assessment process, Jacobian will communicate with the customer both inside and outside of the tool in order to note any gaps, ask for additional information, recommend remediation and advise the customer on factors that may affect validation and certification.

Once the answers to questions and evidence supplied is deemed sufficient to pass, Jacobian will submit the report to HITRUST for validation and QA.

Validation & QA

During this phase, HITRUST will randomly select controls for validation. If there is any additional information or clarification needed, HITRUST will contact Jacobian. Once there is sufficient information to process and QA the submitted data, HITRUST will place the assessment into a queue awaiting assignment to an internal QA auditor. There is no service-level agreement or estimate provided by HITRUST at any time during this process.

At the conclusion of the process, HITRUST will issue a validated report and if the minimum standard have been met, they will issue certification as well. Any controls that are not at least a "3+" in the tool will also generate a corrective action plan for the customer to implement over the coming term.

Validated Report Issued & Interim Assessment

Once a validated report is issued, there will be an interim review required 12 months later. HITRUST expects certified organizations to make progress on the recommended corrective action plans (CAPs) to demonstrate a commitment to a high standard of security and compliance.

When it comes time to conduct the interim assessment, Jacobian will review the controls, assist the customer through the process and submit the information to HITRUST.

At the two-year mark, the customer will undergo a full assessment again and can use the existing data in MyCSF if a subscription has been maintained during the previous 24 months.