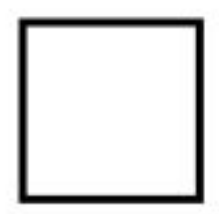# HITRUST Checklist

**Streamline your HITRUST Certification Process**

Gather HITRUST Information

Before getting started, understand who the Health Information Trust Alliance (HITURST) organization is, what they stand for, and which industries they typically work with. HITRUST applies to a variety of industries, but particularly to healthcare.

Head over to the HITRUST website to get an overview of the Cybersecurity Framework (CSF) you'll be working with, download the free PDF, and save it in a designated HITRUST certification folder on your computer to use throughout the process.
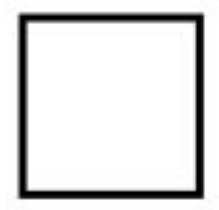
Select an Assessment Level/Audit Type

Work with an authorized CSF assessor to determine which kind of audit makes sense for your business or organization. You'll want to learn about different types of audits, including HITRUST CSF as well as proprietary audit processes available from private auditors.

You'll want to work with your assessor to complete a HITRUST certification assessment not only to give you a better idea of the process but to also perform preliminary tasks like a cybersecurity gap assessment. This will go towards determining the level of HITRUST certification necessary.
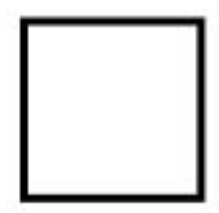
Define the Scope and Cost

This step is all about estimating the time, cost, and internal resources it will likely require to complete your HITRUST certification. This will largely depend on which of the three HITRUST levels you need to comply with, based on your assessment. There are 19 different HITRUST domains, dozens of controls, and more than 700 potential requirements that play into the scope of the project.

To get a better idea of the scope of your assessment prior to getting started, check out the HITRUST MyCSF software-as-a-service tool.
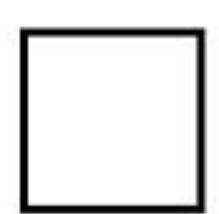
Complete the Framework

This is where the rubber meets the road in terms of documentation. You'll need proof of policies, risk assessments, technical specifications, and any special configurations you might be using.

To determine if your systems and operations are acceptable, you'll need to compare your internal policies, procedures, and audit findings with the requirements list in the myCSF tool. Your first-year audit might take 3-6 months, but only two months for subsequent audits.

Privacy control requirements for HITRUST are on the rise, so make sure that you're informed on the latest changes.
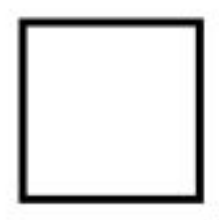
CYBER INSURANCE Keep your business on a stable financial foundation should a cyber security event occur — get cyber damage and recovery insurance today.

HITRUST Checklist

Streamline your HITRUST Certification Process

Validate with an Assessor

Get a professional to check your work. Assessors aren't exactly pushovers, and they'll want to see evidence for anything you provided in your audits. They'll stick to the facts, and their validation will be a big piece of certification. They'll review all of your security and privacy controls, and cybersecurity gaps that you've filled while completing the framework, and recommend any additional steps prior to certifying with HITRUST.

The validation can take four to five weeks.
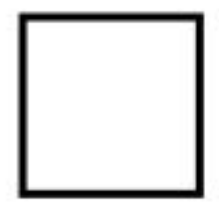
Certify with HITRUST

It will take up to 18 months for HITRUST Alliance lawyers to examine your audit in detail upon submission, and you may be required to submit further information upon request.

HITRUST will typically perform quality assurance procedures, create a report and, depending on the scores in the report, then issue a Letter of Certification. Once approved, proof of compliance is valid for two years, with the expectation that you keep things up to par.

You should then review your work with your assessor, and determine if its the right partner for your next certification or if you might need to look for a new one.

CYBER INSURANCE Keep your business on a stable financial foundation should a cyber security event occur — get cyber damage and recovery insurance today.