securityMETRICS®

HITRUST CSF Preparation Checklist

DEFINING YOUR SCOPE

DETERMINING NEXT STEPS

SELECT HITRUST VALIDATION TYPE

GAP ASSESSMENT / REMEDIATION

CONDUCT FINAL HITRUST CSF ASSESSMENT

HITRUST INTERIM ASSESSMENT

Get a HITRUST Audit →

Note:

This handout aims to assist those who are new to HITRUST. This suggested guideline can help you anticipate your HITRUST tasks. This is not a comprehensive handout, your HITRUST certification steps should be addressed based on how your organization handles sensitive data. A complete list of control requirements can be found here.

Defining Your Scope

The most important step in conducting any type of data security or privacy assessment is to properly understand and define the scope of the systems, people, and processes involved in receiving, handling, and future movement of the data. If this step is done correctly and thoroughly it will set the stage for a successful HITRUST Assessment.

- [ ] **Define and classify protected information your company obtains or generates (e.g., electronic or other media), such as:**
  - [ ] Personally Identifiable Information (e.g., name, address, phone, email, photos)
  - [ ] Demographic information (e.g., race, age, sex)
  - [ ] Medical records (e.g., diagnosis, prescriptions, treatment, research, condition)
  - [ ] Billing Information (e.g., payment info, amounts, SSN, insurance #)
  - [ ] Other sensitive data (e.g., PHI, cardholder information)
- [ ] **Understand how data enters, exits, and moves within your environment**
  - [ ] Meet with each department and identify how various types of protected data enter and are used in their environments by asking:
    - [ ] How do business associates communicate with you?
    - [ ] Are there web pages that collect information?
    - [ ] Is data collected via phone, email, standard mail, fax, data drop, etc.
    - [ ] Where are staff members that enter/process protected data?
    - [ ] Do you receive marketing databases of potential customers to reach out to?
- [ ] **Visualize the volume of protected data being collected/processed in each data flow**
  - [ ] Diagram all protected data flows within your environment
    - [ ] Capture each data flow

Get a HITRUST Audit →

- [ ] Note which departments are involved
- [ ] Pinpoint which systems the protected data traverses
- [ ] Consider backups, recordings, multiple facilities, etc.

- [ ] Identify how various types of protected data exit your environment
  - [ ] Do you send protected data out of your environment?
  - [ ] Characterize in what form the data leaves
  - [ ] Where is the data going?
  - [ ] Do you have agreements with entities receiving protected data you send?

- [ ] Recognize what happens to protected data when it leaves your environment by considering these examples:
  - [ ] Data transfer lifecycle to business associates/third parties
  - [ ] Is data protected during any motion (physical or electronic)? How?
  - [ ] Is the data leaving limited to the minimum necessary information?
  - [ ] Recycling companies / Document disposal
  - [ ] Trash bins on computers

- [ ] **Review system inventories for accuracy and completeness**
  - [ ] Identify servers, network gear, workstations, etc.
  - [ ] Specify the purpose of the hardware and software you use to handle protected information by asking these questions:
    - [ ] How many mobile devices do you have, and who owns them?
    - [ ] Are the attributes of your hardware/software in use tracked? (e.g., versions)

- [ ] **Document where protected data is stored in your environment, including electronic and physical locations, such as:**
  - [ ] Servers
  - [ ] Workstations/computers
  - [ ] Networked medical devices
  - [ ] Laptops
  - [ ] Operating systems (e.g., logs, usernames)
  - [ ] Applications

Get a HITRUST Audit →

- [ ] Encryption software
- [ ] Filing cabinets
- [ ] Personal or company-owned mobile devices
- [ ] Calendar software
- [ ] Email

Determining Next Steps

Now that you know where your data is and what it is doing throughout your environment, you need to confidently decide the right path for your data security/privacy and full compliance to the HITRUST standards.

If you are committed to, or required to become fully HITRUST validated and certified, you can proceed to the “Select HITRUST Validation Type” section of this checklist.

If you are not quite ready to commit to the cost of the MyCSF portal but want to progress towards better security and privacy for your organization, go to the “Healthcare Security Foundation” section at the bottom of this checklist.

Select HITRUST Validation Type

Now that you have chosen to go through the formal HITRUST CSF pathway, it is important to determine the type of HITRUST validation you want to work towards. It may be that you start with one and move to another during this process.

- [ ] Contact HITRUST to purchase access to MyCSF portal
  - [ ] Upload the necessary documents for your HITRUST Assessment
  - [ ] Review the specific requirements and align your organization’s goals accordingly
  - [ ] Complete scoping exercise in MyCSF portal to prepare for questions about:
    - [ ] Organization size
    - [ ] Number of applications that use protected data
    - [ ] Number of transactions that occur with protected data

Get a HITRUST Audit →

- [ ] Examine your scope and organizational capabilities
  - [ ] Determine which key business stakeholders can facilitate the adoption of the HITRUST CSF within your organization

[ ] Decide which type of HITRUST Assessment that you will prepare for, including:

- [ ] HITRUST Readiness Assessment
  - [ ] Consider this assessment type if your main goal is to identify security gaps before paying another company to do a HITRUST CSF Validated Assessment
    - [ ] Use MyCSF portal to complete your readiness assessment
      - [ ] Work with a HITRUST consultant to check your work
- [ ] HITRUST CSF Validation Assessment
  - [ ] Consider this assessment type if you'd like to become HITRUST CSF Validated, which entails working with a certified assessor to verify that security controls are in place
    - [ ] Use MyCSF Portal to record your status
      - [ ] Engage a HITRUST CSF external assessor
      - [ ] External assessor gathers evidence and forms opinion and enters that into MyCSF portal
      - [ ] If you fail your HITRUST CSF Validation, consider next steps
      - [ ] If you qualify, consider continuing on to be HITRUST CSF Certified
        - [ ] Submit data on MyCSF portal to HITRUST for validation and certification

[ ] HITRUST CSF Certified

- [ ] Consider this assessment type if you want to become HITRUST CSF Certified, which entails working with a certified assessor to individually review and score each of your organization's security measures
  - [ ] Use MyCSF Portal to record your status
    - [ ] Engage a HITRUST CSF external assessor
      - [ ] External assessor gathers evidence and forms opinion and enters that into MyCSF portal
        - [ ] Submit data on MyCSF portal to HITRUST for validation and certification

Get a HITRUST Audit →

Gap Assessment / Remediation

No matter what type of HITRUST Assessment is chosen it is a good idea to evaluate the maturity of your processes against your set of HITRUST controls. This can be done by conducting a gap assessment and remediating any negative findings before completing your HITRUST process.

- [ ] Choose who will conduct your HITRUST Assessment:
  - [ ] Internal resources can be used to conduct a HITRUST Readiness Assessment
  - [ ] HITRUST CSF external assessor(s) will conduct the gap assessment for a validated or certified assessment
- [ ] Conduct a gap assessment against all controls determined in the MyCSF portal
- [ ] Remediate any findings that were identified during your gap assessment
  - [ ] Plan for issues that will take more time, such as properly implementing data encryption
  - [ ] Resolve high-risk issues first
  - [ ] Work with your internal team or third-party assessor to ensure controls have been implemented as intended to comply with HITRUST CSF

Conduct Final HITRUST CSF Assessment

Once you've conducted a gap assessment and made the necessary remediation changes, it's time to conduct the final HITRUST CSF Assessment.

- [ ] Ensure that you have made all changes to documentation (i.e., policy and procedures)
- [ ] Certify that you can demonstrate that all policies and procedures have been in place for at least 90 days
- [ ] Begin formal HITRUST Assessment
  - [ ] Work with internal staff or HITRUST CSF Assessor firm to record responses in MyCSF portal for each control

Get a HITRUST Audit →

- [ ] Assign a score to it based on your own evaluation of your compliance
  - [ ] Must evaluate each control in accordance with the HITRUST CSF scoring rubric
- [ ] Upload your evidence to the portal as needed

- [ ] Finalize details with HITRUST to receive your final report

HITRUST Interim Assessment

An interim assessment will be required if you have chosen to conduct a HITRUST CSF Certified assessment (which is valid for two years). This will be due at the one year mark after your first certified assessment.

- [ ] Plan for the required interim assessment at your one-year mark
  - [ ] Engage HITRUST assessor to conduct your interim assessment
    - [ ] Be aware that your interim assessment will be created by HITRUST and will be available for 120 days before your one-year anniversary date
  - [ ] Submit interim assessment
- [ ] Maintain compliance throughout your two years

Additional Preparation:

Healthcare Security Foundation (HSF) Assessment

This is a general “best practice” security and privacy assessment that is based on the popular CIS Controls and HIPAA rule privacy guidelines. Controls contained in this foundational assessment will help a company establish industry-standard security and privacy practices as you prepare for a full HITRUST Assessment.

- [ ] Work with your assessor to conduct a gap assessment that will check your current security and privacy controls to the HSF requirements
- [ ] Remediate deficiencies
- [ ] Conduct final HSF Assessment
- [ ] Review your results

Get a HITRUST Audit →

Interested in a HITRUST CSF Assessment?

Request a Quote Now →

Get a HITRUST Audit →

© 2021 SecurityMetrics

securityMETRICS®