AMPCUS CYBER

Zero Trust Compliance Service Provider

Step-by-Step Guide to a Successful HITRUST Certification

Introduction

Obtaining a HITRUST certificate is not an easy job. It involves extensive preparation, a rigorous assessment process, and ongoing commitment. Additionally, the process flow requires a significant amount of upfront work, including documenting compliance, fixing identified weaknesses, and potentially implementing new systems and policies. Ultimately, this can be overwhelming and cause fatigue, or sometimes lead to confusion, slowing down the certification process. Often, these challenges can cause the organization to extend its timeframe for assessment, mitigation, and audit.

Additionally, maintaining certification requires periodic reassessment and staying current with framework changes.

To solve these challenges, organizations must rely on HITRUST-authorized assessors who come with extensive knowledge and experience to streamline the certification journey by implementing the right processes, security controls, and policies related to HITRUST CSF. Speaking in that light, Ampcus Cyber provides one of the best-in-class assessors who not only understand your requirements but also act as strategic partners.They bring deep expertise to the table, identifying gaps proactively and guiding your firm toward full compliance with all required regulatory standards. With Ampcus Cyber, organizations gain a clear understanding of the HITRUST assessment process, including well-defined roles and responsibilities for both parties. Here's a comprehensive guide to our approach.

Entities involved in the
HITRUST Assessment Process

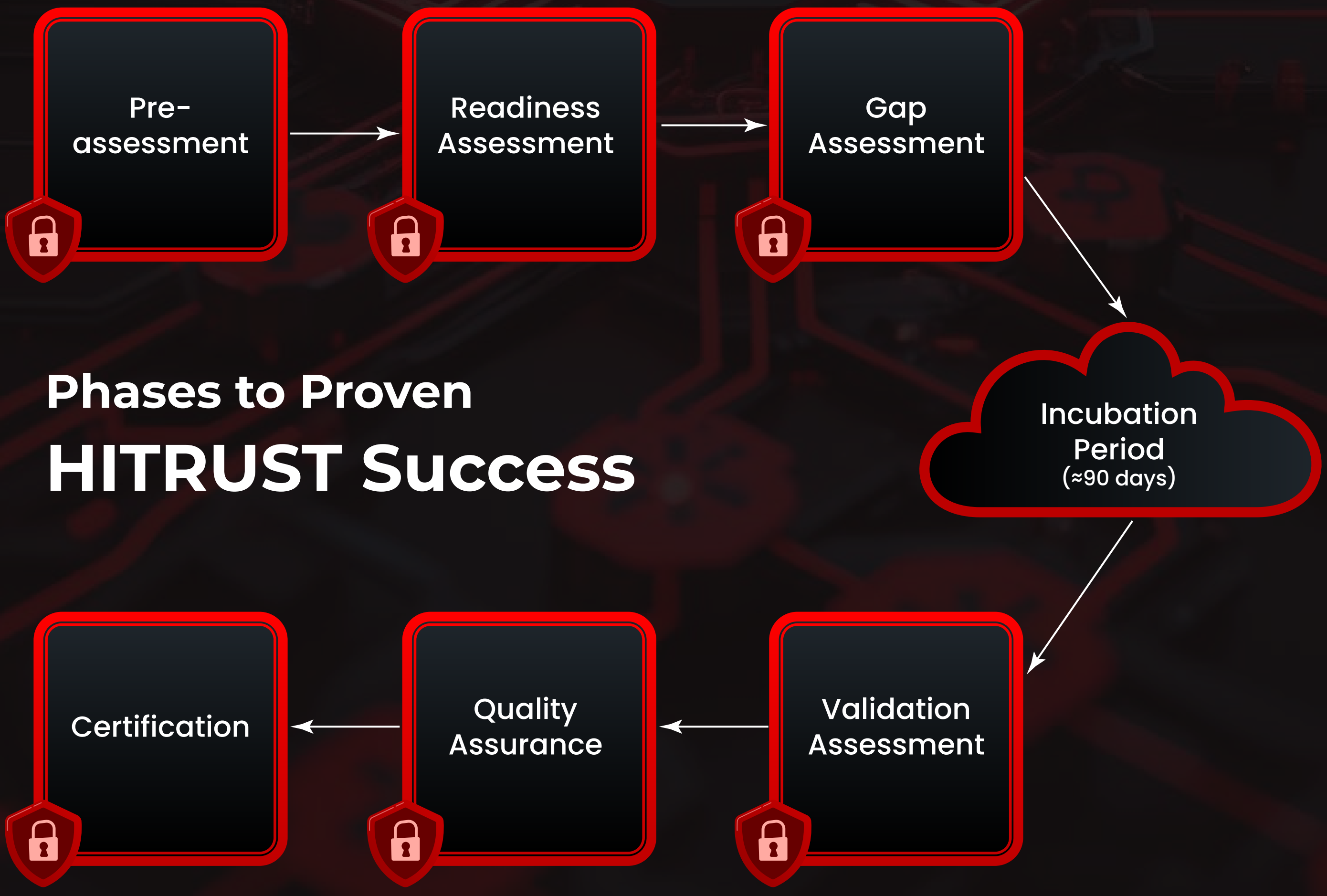
- **Assessed entity:**
  This is an organization - such as a healthcare provider, payer, or business associate - undergoing a HITRUST assessment. The organization is responsible for implementing the necessary security and privacy controls.

- **HITRUST-certified assessors:**
  They are responsible for validating the scope defined by the client/ śorganization and conducting validated assessments. They evaluate the entity's security controls, identify gaps, and document the findings, in addition to assisting the organization in uploading the assessed details to the MyCSF portal.

- **HITRUST:**
  The Health Information Trust Alliance is the organization that develops and maintains the HITRUST CSF, certifies assessors, and provides quality assurance for the assessment process. HITRUST also issues the final certification upon successful completion of the validated assessment.

- **MyCSF:**
  It is a trusted platform from HITRUST that acts as a central hub for uploading details related to assessment and managing information and compliance.

Phases to Proven
HITRUST Success



Pre-assessment

Readiness Assessment

Gap Assessment

Incubation Period (≈90 days)

Validation Assessment

Quality Assurance

Certification

Pre-assessment Phase

The phase starts with the organization sharing necessary details through questionnaires from the assessor. These details include the preferred assessment type (e1, i1, and r2), company background, business operations, and the scope of the assessment. Once the pre-assessment stage is completed, the process moves to **Readiness Assessment,** followed by a **Validated Assessment.**

It is not necessary that every organization seeking HITRUST certification must go through a Readiness Assessment. Depending on the current security posture and compliance maturity, they can move straight to the Validated Assessment. This saves both time and resources.

Readiness Assessment Phase

It is a process that helps the organization understand and evaluate its preparedness for achieving HITRUST certification. The assessment can be done by oneself or involve HITRUST-certified assessors.

Purpose

- It helps the organization identify weaknesses and control before official submission.
- It helps to familiarize the organization with HITRUST CSF requirements.
- It reduces surprises or delays during the Validated Assessment.
- It guides remediation planning to align with HITRUST controls.
- It improves audit readiness and internal confidence.

Workflow

Here's a detailed breakdown of the Readiness Assessment workflow.

1. Kickoff Meeting & Scoping:

- This initial phase establishes timelines, points of contact, and provides a general overview of the organization.
- It's also when the key stakeholders get training about the importance and benefits of the HITRUST certificate. With the help of an assessor, the scope of the assessment is defined, including the size of the organization, data volume, and systems involved.
- As part of the scoping process, the organization completes a detailed questionnaire that matches those on the HITRUST MyCSF portal.
- The questionnaire helps identify the organization's specific compliance needs based on its attributes and risks.

2. Gap Analysis and Remediation:

- Based on the responses, a detailed gap analysis is conducted to evaluate their current implementation and provide detailed responses. This includes documenting if a policy or standard is in place and if the control is effectively implemented.
- Based on the evaluation and responses, a maturity level to each control is assigned, highlighting areas where the organization falls short of HITRUST requirements. This gives the maturity score of the organization, ranging from non-compliant (0%) to fully compliant (100%).
- Strategies for improvement are then developed and implemented to address these gaps.

3. Preparing for Validated Assessment:

- The Readiness Assessment provides a strong foundation for the subsequent Validated Assessment, which is required for HITRUST certification.
- By identifying and addressing gaps early on, the organization can streamline the validation process and increase their chances of success.

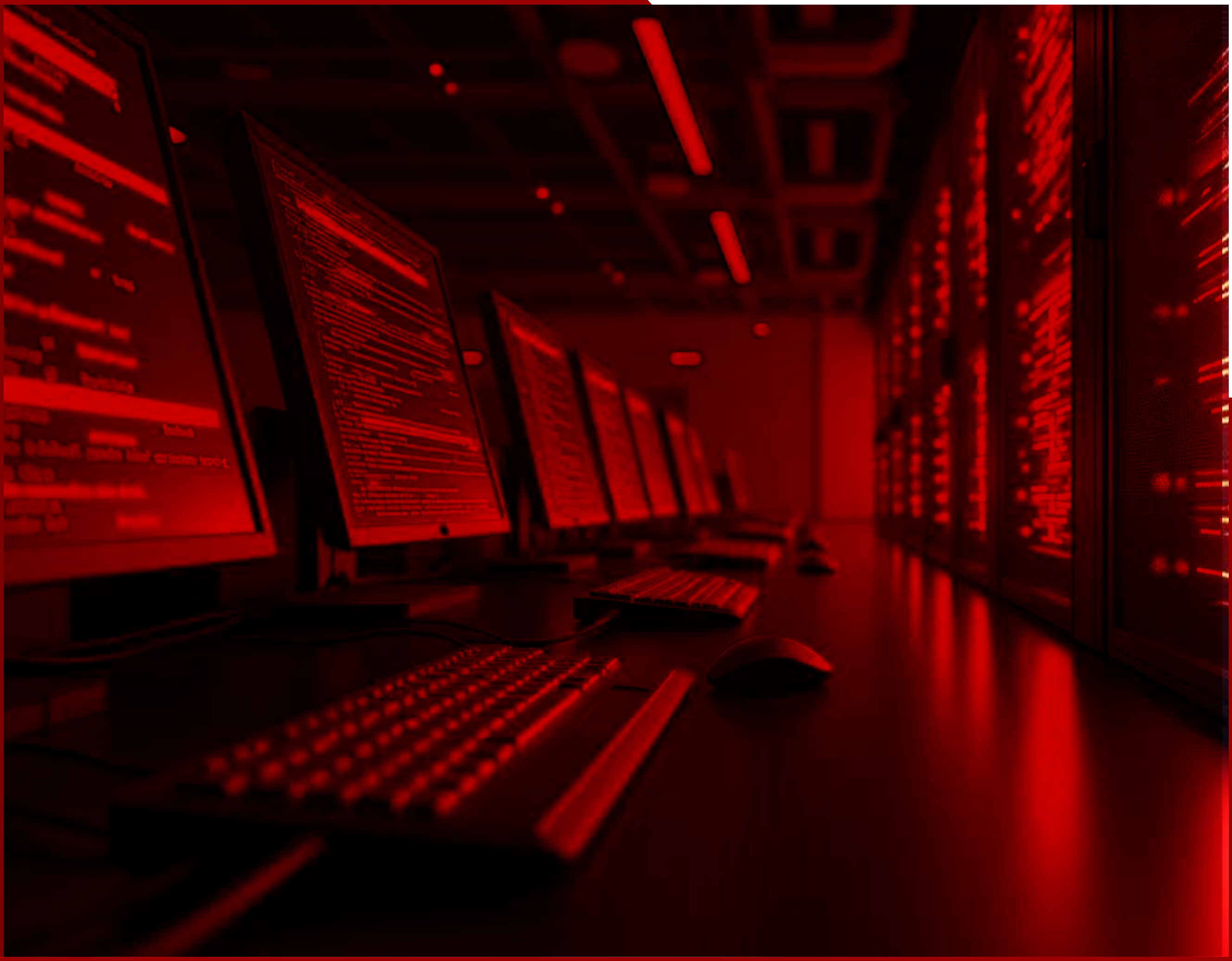
Note: **Based on the risk profile,** *company size, and assessment level opted, this process can be between* **50-70 days.**

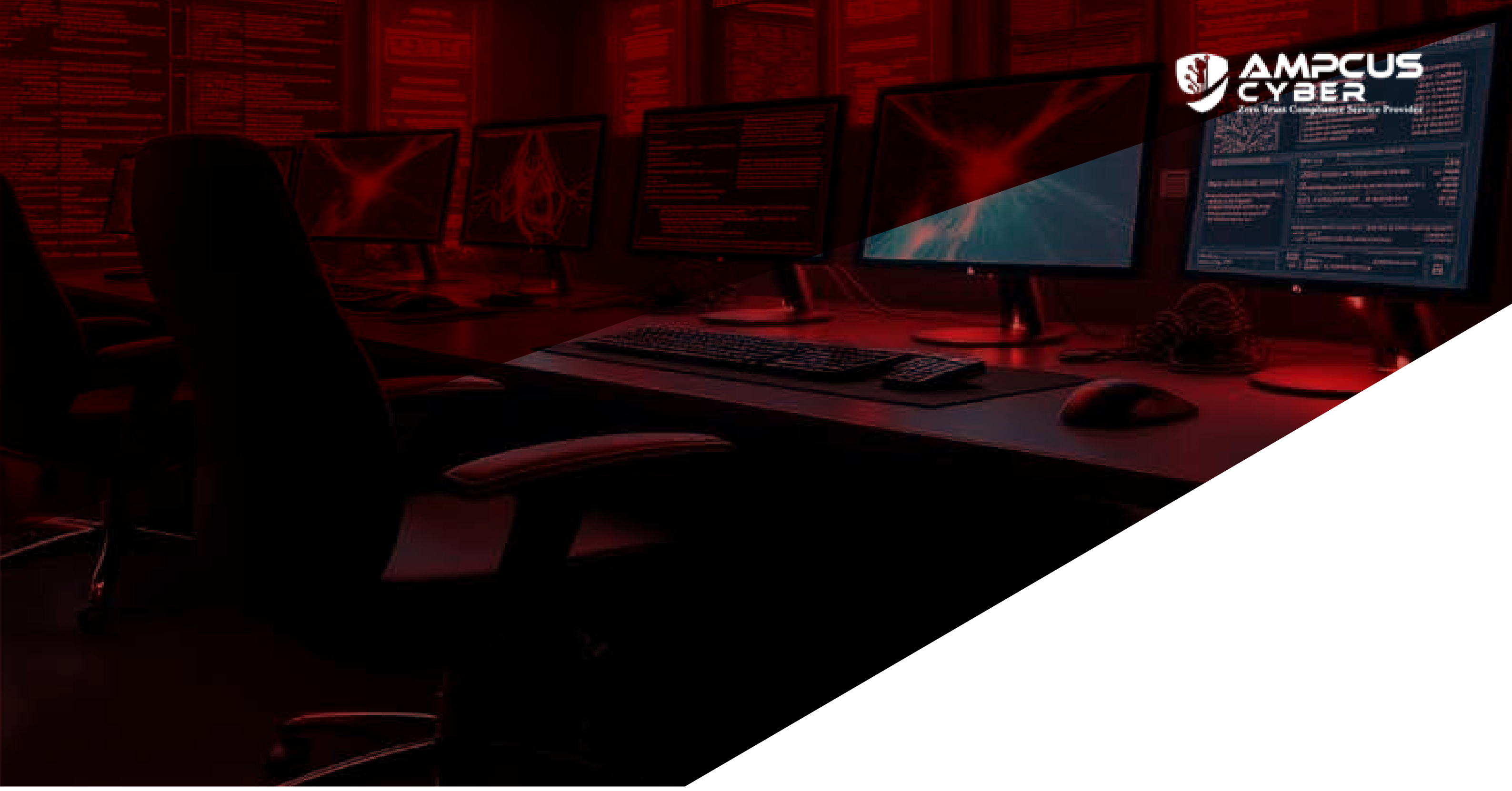
Validation Assessment Phase

It is a mandatory assessment required for organizations seeking HITRUST certification. It involves a detailed evaluation of an organization's implementation of security and privacy controls based on the selected HITRUST CSF assessment level (e1, i1, or r2).

Purpose

- It assures that an organization has implemented the required controls and policies effectively.
- It enables the organization to initiate the formal submission to HITRUST for potential certification.
- It helps organizations to mitigate third-party risk by validating compliance through an independent assessor.
- It also fosters improvement in the organization's security program.





Workflow

Here's a detailed breakdown of the Readiness Assessment workflow.

1. **Sample Selection, Evidence Collection and Submission:**

- Assessors scrutinize all aspects of the assessment to determine whether controls meet the required standards.
- A detailed population request list is shared with the organizations. This includes mapping data flows, identifying involved departments, and analyzing systems that process protected data.
- A secured collaboration and communication channel is established between the client and assessor for questions and clarifications. This channel serves as the central point for timely queries, clarifications, and ongoing coordination between the client and assessment teams.

2. **Control Validation and Evidence Submission to MyCSF**

- Assessor validates the submitted evidence against HITRUST requirements across all three elements - policies, procedures, and implementations. This validation is performed using the illustrative procedures provided within the MyCSF platform, ensuring alignment with HITRUST's defined expectations.
- All observations are documented with precision and clarity. Assessor follows a standardized approach to writing comments, ensuring each observation clearly explains how the evidence meets (or does not meet) the specific control requirements.
- Once the organization submits all assessment domains to the assessor, the assessment enters the Performing Validation phase. The assessed details are uploaded to the MyCSF portal.

Note: **It takes between 90-120 days before the final submission. It is important to note that HITRUST r2 Validated Assessment is the most comprehensive assessment and repeats every two years with an interim period in between.**

Quality Assurance Phase

Assessor conducts a rigorous QA review of the submitted assessment in MyCSF on behalf of the organization, ensuring compliance with HITRUST standards and requirements. As part of the review, they assist the organization in resolving any identified discrepancies or queries on the portal by providing supporting documents or answers as needed.

Once all tasks are completed and accepted by HITRUST, a compliance certificate is issued.

END