AMPCUS CYBER
Zero Trust Compliance Service Provider

HITRUST CSF

A Comprehensive Guide To e1, i1, and r2 Assessments

Introduction

No organization is immune to cyberattacks. From ransomware attacks to data breaches, the threat landscape is growing in scale and complexity. This puts organizations at risk of cyberattacks more than ever, increasing the chances of sensitive information getting into the wrong hands. As technology advances, cybercriminals evolve, adopting smarter, stealthier approaches to outpace traditional defenses.

To stay ahead of these threats, organizations must answer two pivotal questions:

- How can they mitigate risks and keep up with evolving security and privacy regulations?
- How can they earn the trust of those who rely on them to keep their data secure?

The answer to both questions lies in the **HITRUST CSF**. HITRUST Common Security Framework (CSF) is a comprehensive security framework that helps organizations, especially those handling sensitive information, manage cyber risks and meet compliance requirements effectively.

The sensitive data includes personal health information (PHI) and other regulated data types associated with the organization. The framework integrates various crucial standards like HIPAA, NIST, GDPR, ISO 27001, and PCI DSS, making it easier for organizations to choose standards per their security posture or country-specific regulatory requirements.

At Ampcus Cyber, we understand the importance of this robust framework, thus enabling organizations to implement the right security controls, policies, and procedures across their infrastructure to ensure compliance and strengthen their overall security posture.

Our Offerings

(HITRUST e1, i1, and r2 Assessments)

Organizations can choose from the following three HITRUST assessment levels based on their operational needs, risk profile, and data flow requirements. These assessments are conducted across 14 control categories, which include areas such as Information Protection Program, Endpoint Protection, Configuration Management, Network Protection, and Access Control.

HITRUST CSF
14 control categories

01 Information Security Management Program

02 Access Control

03 Human Resources Security

04 Risk Management

05 Security Policy

06 Organization of Information Security

07 Compliance

08 Asset Management

09 Physical and Environmental Security

10 Communications and Operations Management

11 Information Systems Acquisition, Development, and Maintenance

12 Information Security Incident Management

13 Business Continuity Management

14 Privacy Practices

These 14 broad control categories encompass 19 specific control domains, with a total of 156 control references mapped to different regulatory and industry standards.

AMPCUS CYBER
Zero Trust Compliance Service Provider

HITRUST CSF
Hierarchical Structure

Over **1900** Requirement Statements

↓

Up to **3** Implementation Levels

↓

156 Control References

↓

49 Control Objectives

↓

14 Control Categories

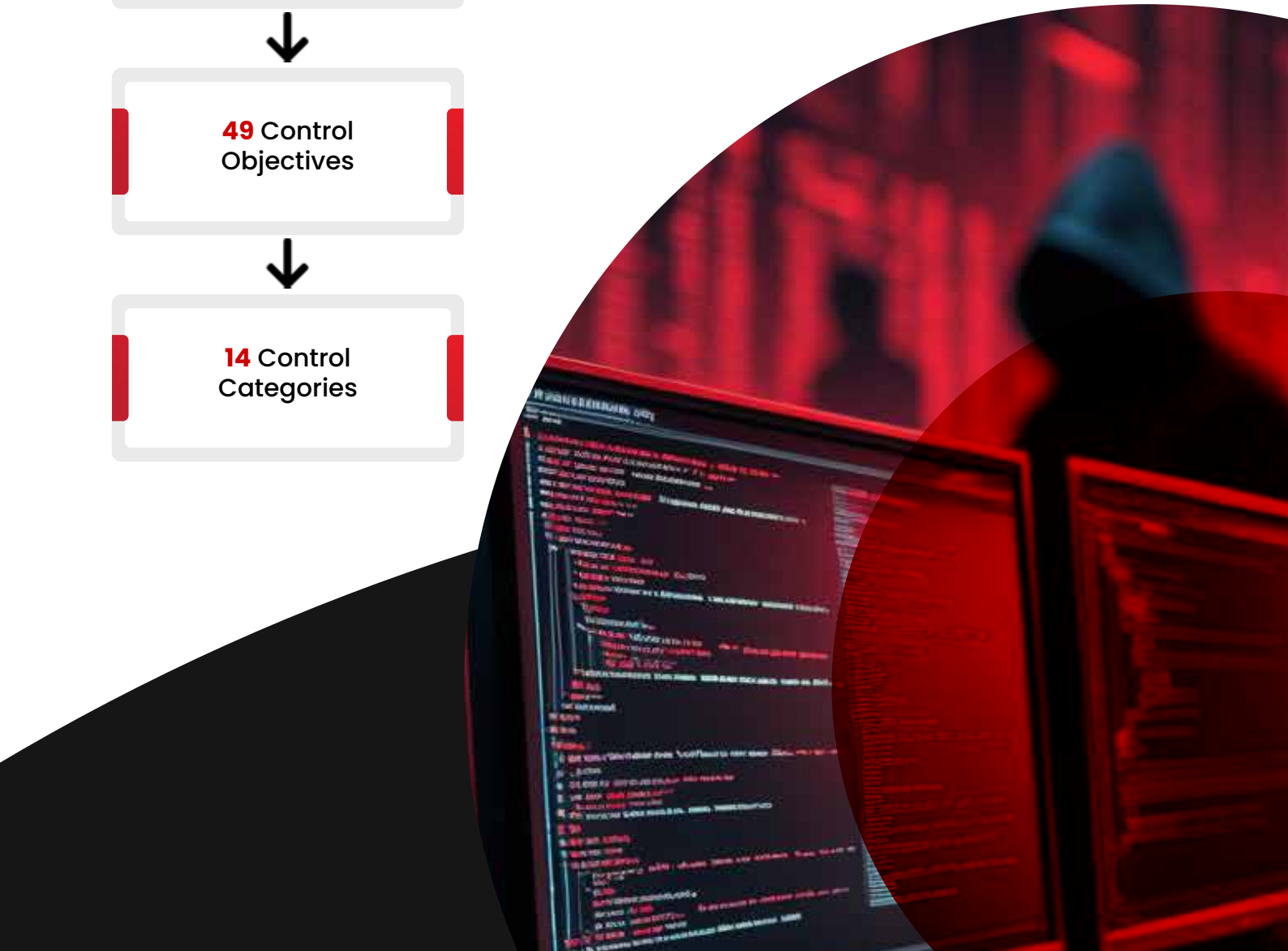
The three assessment levels are:

HITRUST e1 (Essential): It is ideal for early-stage firms or vendors looking to prove due diligence in third-party assessments.

HITRUST i1 (Implemented): It offers a moderate level of assurance and is suitable for organizations looking for more robust information security programs. It strikes the right balance between cost and rigor for growing firms managing vendor ecosystems.

HITRUST r2 (Risk-based): It is a rigorous assessment, suitable for organizations with high-risk profiles or those needing to comply with multiple regulatory standards.

Each assessment builds on the previous one, allowing organizations to scale their cybersecurity efforts as their needs evolve.



Key Characteristics of e1 (Essential)

- The HITRUST e1 Assessment, ideal for startups and companies with low risk profiles, includes 44 foundational security controls across different domains.
- The 44 security controls included in HITRUST e1 address the most pressing active cyber threats, such as phishing and ransomware, thus enabling organizations to maintain good cybersecurity hygiene.
- The e1 Assessment can be performed as a Readiness or Validated assessment. The Readiness assessment can be self-assessed or facilitated by an external assessor.
- While Readiness assessment helps stakeholders within an organization understand how well they are prepared for the e1 Validated assessment and certification, an e1 certificate is only issued if the organization opts for the Validated assessment.
- A HITRUST e1 certification is valid for one year, after which the organization must undergo a Recertification Validation Assessment to maintain its e1 certificate.
- Some of the use cases of the e1 certificate include ensuring baseline cybersecurity practices, preparing for more robust HITRUST assessments, and building trust with customers as a startup.

Key Characteristics of i1 (Implemented)

- Suitable for mid-level organizations, i1 Assessment offers a more comprehensive level of assurance as compared to e1, with more controls in scope.
- Designed to include third-party management, the assessment is done across 187 controls, including the 44 from the e1 assessment.
- The i1 Assessment can be performed as a Readiness or Validated assessment. The Readiness assessment can be self-assessed or facilitated by an external assessor.
- The purpose and nature of the Readiness assessment in i1 are the same as e1 and do not include third-party review. An organization is eligible for a one-year certificate only after undergoing a Validation assessment, after which it has to follow the recertification process to renew the i1 certificate.
- It is useful for organizations developing/supporting third-party risk management (TPRM) or preparing to scale towards the HITRUST r2 certification process.

Key Characteristics of r2 (Risk-based)

- It fits well for organizations that need to comply with multiple authoritative sources, such as HIPAA, NIST, ISO 27001, and PCI DSS, or require expanded control tailoring based on identified risk factors.
- Unlike e1 and i1, which include a fixed set of controls, the r2 assessment is tailored using a risk assessment questionnaire. While there are over 2,000 possible controls, a typical r2 assessment averages around 385 controls.
- The certificate is valid for two years, and after a year, the organization needs to go through an interim assessment to verify if its controls still meet requirements, e1 and i1 requirements . The interim assessment also ensures continued compliance with controls established during the initial assessment.
- The certification provides the highest level of HITRUST certification, ensuring compliance in highly regulated business environments.

AMPCUS CYBER
Zero Trust Compliance Service Provider

HITRUST Certification Process

1 Readiness
(up to 2 months)

- Identify the key stakeholders
- Define the score
- Select an authorized external assessor organization
- Readiness Assessment

2 Remediation
(up to 3-4 months)

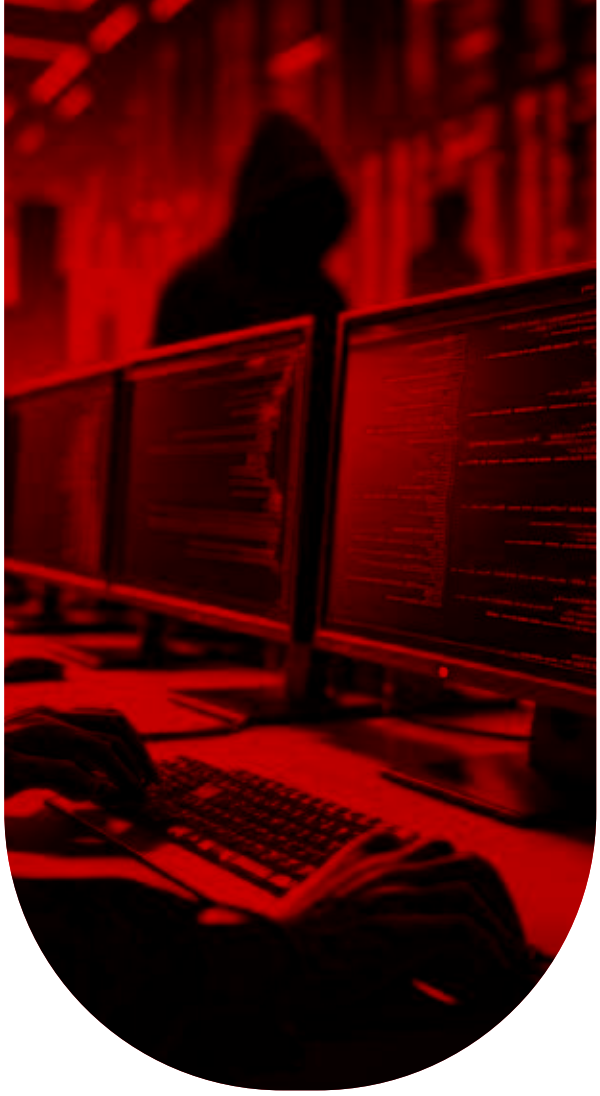
- Gap Analysis
- Develop Remediation Plan
- Set a time for the Validated Assessment

3 Validated Assessment
(up to 3 months)

- Complete the Validated Assessment using the MyCSF tool
- The assessor validates and audits the assessment

4 HITRUST Quality Assurance Review
(1 to 2 months)

- HITRUST will perform the required quality assurance procedures
- HITRUST will create a report and score the validated assessment
- HITRUST will issue a Letter of Certification



Choose Best-in-Class Experts to Achieve Your Goal

Whether it is finalizing the certification requirements or validating the assessment, Ampcus Cyber's HITRUST authorized assessors are here to help your organization navigate easily through the certification process. The assessors will:

- Guide you through scoping, control selection, and certification planning
- Conduct readiness reviews to identify gaps
- Assist in uploading comprehensive information to the MyCSF portal for managing HITRUST CSF certification process
- Recommend the most cost-effective and appropriate assessment level

END