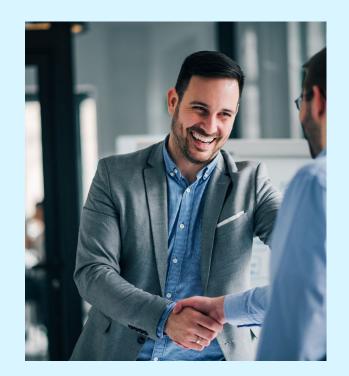# How HITRUST Helps Organizations Manage Risk

CHALLENGE …

Organizations today are facing a **new, universal CHALLENGE.**

Access to **capital and customers** is increasingly becoming a **QUESTION OF CONFIDENCE.**

Stakeholders want **assurances** toward little or **NO RISK.**

Customers want **assurances** toward **DATA PROTECTION.**

It is an **ENORMOUS, COMPLEX, AND COSTLY** challenge for organizations to provide these **assurances.**

You are focusing on driving your business.

Who is focused on protecting it?

HITRUST®

It may be time to think about implementing a comprehensive information **risk management and compliance program.**

Are we addressing applicable state, federal and international regulations?

What metrics are we using to measure ourselves against comparable organizations?

How do we select a program that scales within our organization?

What is the most effective way to evaluate the effectiveness of our third parties' privacy and security controls?
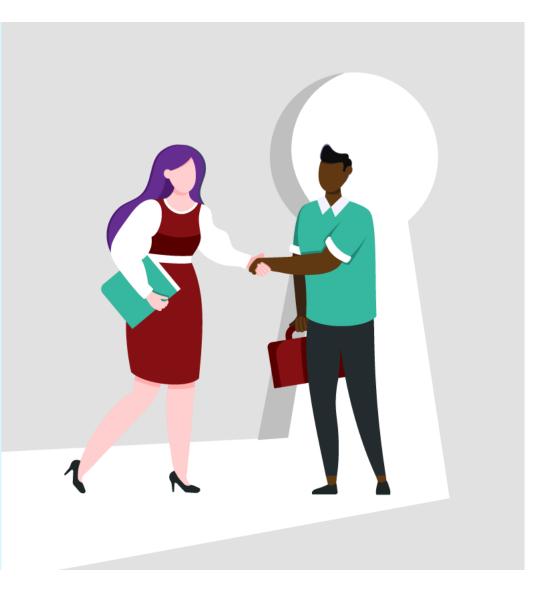
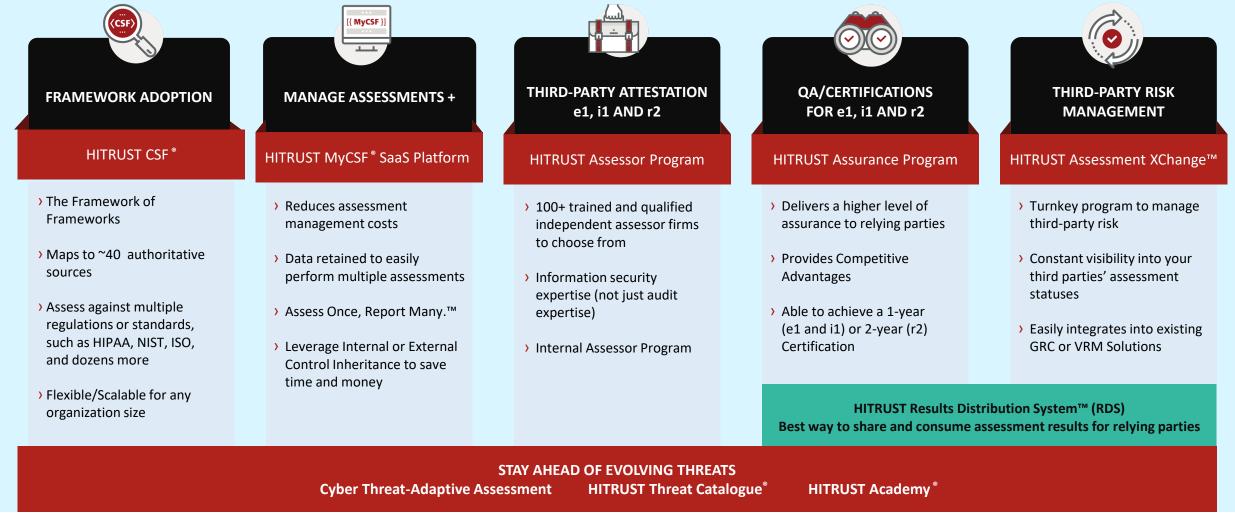**HITRUST**®

HITRUST Can Help

HITRUST

Champions programs and solutions that protect sensitive information and manage information risk and compliance, from start to finish, for organizations across all industries.

All the Programs and Tools You Need in One Spot — The HITRUST Approach

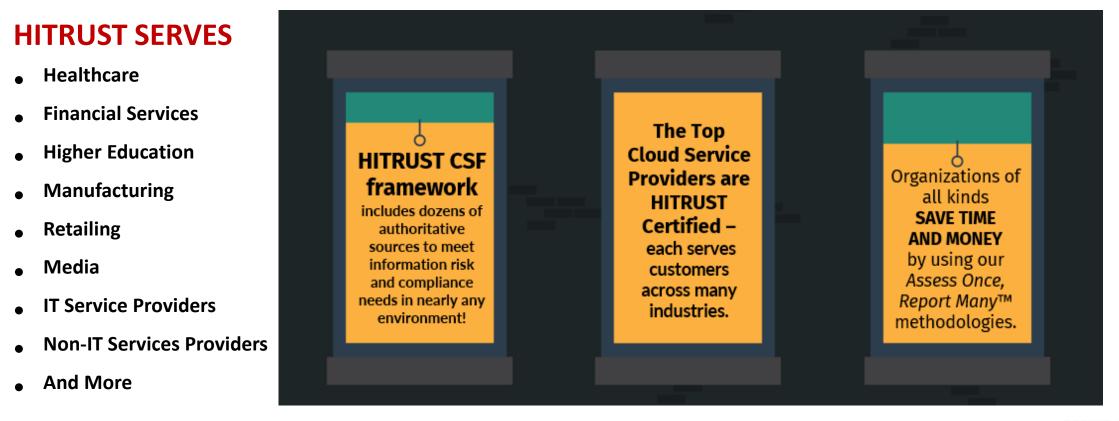**The best choice for your organization's information risk management and compliance program.**

FRAMEWORK ADOPTION	MANAGE ASSESSMENTS +	THIRD-PARTY ATTESTATION e1, i1 AND r2	QA/CERTIFICATIONS FOR e1, i1 AND r2	THIRD-PARTY RISK MANAGEMENT
HITRUST CSF ®	HITRUST MyCSF ® SaaS Platform	HITRUST Assessor Program	HITRUST Assurance Program	HITRUST Assessment XChange™
› The Framework of Frameworks	› Reduces assessment management costs	› 100+ trained and qualified independent assessor firms to choose from	› Delivers a higher level of assurance to relying parties	› Turnkey program to manage third-party risk
› Maps to ~40 authoritative sources	› Data retained to easily perform multiple assessments	› Information security expertise (not just audit expertise)	› Provides Competitive Advantages	› Constant visibility into your third parties' assessment statuses
› Assess against multiple regulations or standards, such as HIPAA, NIST, ISO, and dozens more	› Assess Once, Report Many.™	› Internal Assessor Program	› Able to achieve a 1-year (e1 and i1) or 2-year (r2) Certification	› Easily integrates into existing GRC or VRM Solutions
› Flexible/Scalable for any organization size	› Leverage Internal or External Control Inheritance to save time and money			

HITRUST Results Distribution System™ (RDS)
Best way to share and consume assessment results for relying parties

STAY AHEAD OF EVOLVING THREATS

Cyber Threat-Adaptive Assessment   **HITRUST Threat Catalogue®**   **HITRUST Academy®**

HITRUST®

HITRUST Helps a Broad Range of Organizations Build Trust and Earn New Business

Our solutions reduce cybersecurity risk and streamline compliance for enterprises across multiple sectors.

HITRUST SERVES

- **Healthcare**
- **Financial Services**
- **Higher Education**
- **Manufacturing**
- **Retailing**
- **Media**
- **IT Service Providers**
- **Non-IT Services Providers**
- **And More**

HITRUST CSF framework includes dozens of authoritative sources to meet information risk and compliance needs in nearly any environment!

The Top Cloud Service Providers are HITRUST Certified – each serves customers across many industries.

Organizations of all kinds **SAVE TIME AND MONEY** by using our *Assess Once, Report Many™* methodologies.

HITRUST®

To improve trust and mitigate data breaches, HITRUST® addresses the globally growing need for a common, comprehensive framework.

The HITRUST CSF

One of the most widely adopted frameworks— maps to dozens of authoritative sources.

HITRUST®

No Matter Your Industry, the HITRUST CSF Includes a Wide Array of Standards, Frameworks, and Regulations

CURRENT AUTHORITATIVE SOURCES INCLUDED IN THE HITRUST CSF v11:			
1 TAC 15 390.2	EHNAC	ISO/IEC 27001:2013	OCR Guidance for Unsecured PHI
16 CFR 681	EU GDPR	ISO/IEC 27002:2013	OECD Privacy Framework
201 CMR 17.00	FedRAMP	ISO/IEC 29100:2011	PCI DSS v3.2.1
21 CFR 11	FFIEC IS Handbook	MARS-E v2	PDPA (Singapore)
23 NYCRR 500	HICP	NIST Cybersecurity Framework v1.1	South Carolina Insurance Data Security Act. (SCIDSA)
AICPA TSP 100	HIPAA Breach Notification Rule	NIST SP 800-171 r2	The Joint Commission v2016
APEC	HIPAA Privacy Rule	NIST SP 800-53 r4	
CCPA 1798	HIPAA Security Rule	NIST SP 800-53 r5	
CIS Controls v7.1	HITRUST De-ID Framework v1	NRS 603A	
CMS ARS v3.1	IRS Pub 1075 (2016)	NYS DOH SSP v3.1	
COBIT 5	ISO 27799:2016	OCR Audit Protocol (2016)	

HITRUST

HITRUST CSF v11: Delivers More Efficiency; Cyber Threat Relevance

Delivers Cyber Threat-Adaptive Assessments

Framework and controls leverage threat intelligence information to proactively defend against the latest cyberthreats, including ransomware and phishing.

Expands and Aligns Assessment Portfolio

Single approach that covers broad assurance needs for different risk levels and compliance requirements providing greater assurance reliability than other assessment options.

Enables Traversable Assessment Journey

Reuses the work in lower-level HITRUST assessments to progressively achieve higher assurances by sharing common control requirements and inheritance.

Reduces Level of Effort

The controls selection and specification ensure the most relevant controls are in place while removing redundancy and can decrease the time and effort toward HITRUST certification.

Expands Authoritative Sources

Updates powered by the speed, efficiency, and automation of Artificial Intelligence (AI).

MyCSF OVERVIEW

Our SaaS Platform, MyCSF® Will Help You Do It All!

The HITRUST MyCSF® is an efficient, easy-to-use platform solution that supports an organization's cybersecurity needs in an ever-changing threat and regulatory environment.

MyCSF enables organizations to perform information security assessments and evaluate compliance coverage for dozens of authoritative sources and industry standards in the HITRUST CSF® framework including HIPAA, NIST 800-53, NIST AI RMF v1.0, NIST Cybersecurity Framework, ISO 27001, FedRAMP, PCI, GDPR, and more.

MyCSF allows organizations to identify requirement statements, establish control scoring, archive supporting evidence, and submit assessment data to the HITRUST Assurance Program™ for evaluation, validation, and certification.

HITRUST®

Hundreds of Thousands of Security Risk Assessments Performed

Building and running a robust information risk management program can be overwhelming, resource-intensive, and costly.

For many organizations, effectively managing this risk is a complex and ever-changing process, often met with confusion and stress.

HITRUST streamlines this process for you, making it *easier than ever* to ensure that sensitive information is protected effectively and efficiently.

HITRUST®

Three Cybersecurity Assessment Levels to Meet Nearly Any Need

HITRUST Assessment Portfolio Features

e1 HITRUST Essentials, 1-Year Assessment

Focused on Foundational Cybersecurity Hygiene

For lower-risk organizations validating the most critical cybersecurity controls.

i1 HITRUST Implemented, 1-Year Assessment

Focused on Leading Security Practices

For organizations with robust information security programs ready to demonstrate implementation of controls that protect against current and emerging threats.

r2 HITRUST Risk-Based, 2-year Assessment

Focused on Expanded Capabilities

For organizations to demonstrate regulatory compliance against authoritative sources such as HIPAA, the NIST Cybersecurity Framework, and dozens of others, or requiring expanded tailoring of controls based on identified risk factors.

Assessment Portfolio Designed to Support an Efficient Path to Program Maturity

One Framework, Assurance Program, and Assessment Tool to Meet the Information Protection Needs of the Entire Enterprise.

3 HITRUST Certification Options
For varying levels of budget, resources, and risk

r2
Expanded Practices

i1
Leading Security Practices

e1
Essentials

Control Nesting Facilitates a Seamless, Efficient, and Progressive Assessment Journey to Demonstrate Growing Security Capabilities

New Entry-Level Essentials (e1) Assessment focused on the most essential and foundational cybersecurity controls -- *An excellent starting point for enterprises early in their program maturity, or as the final assurance destination for low-risk organizations.*

Unique Assessment Portfolio Design supports an efficient path to program maturity by sharing common controls that build on each other -- *Simplifies the journey toward stronger security capabilities and assurances and is ideal for managing third-party risk allowing progressive steps your vendors can take toward a targeted assurance.*

Efficiency Innovations including control nesting, internal/external control inheritance, and rapid recertification -- *Make the assessment process faster and easier to perform.*

HITRUST®

HITRUST Certification Provides a Competitive Advantage

"You get the credibility, we improved our business processes, and we were able to reduce our cybersecurity insurance costs."

—*CFO & CCO, technology services organization, NJ*

"Approximately 40-50% of the prior year's revenue was due to our organization's HITRUST CSF Certification."

—*CISO, technology organization, WI*

"Our company recouped our investment in getting certified within 30 days."

—*CEO, healthcare IT startup, CA*

"We find great value in using the framework to make sure our IT systems protect the sensitive information of the organization and our patients."

—*Sr. Mgr. of Cybersecurity, network of hospitals for children, FL*

"I have security and risk conversations with my peers, the board, the executive team, the CTO and the CSO. The CSF is a great tool for getting everyone onto the same page."

—*Sr. Director of Security Strategy, financial technology services organization, WI*

"We can even provide a certification score to prove our level of maturity around the NIST cybersecurity framework; that's a feature that most other common frameworks do not provide."

—*VP of Information Security & Privacy, healthcare provider & insurer, PA*

HITRUST

Starting Your Journey to HITRUST Certification

1

DOWNLOAD THE HITRUST CSF FRAMEWORK

Identify your security and privacy controls.

2

CONDUCT A HITRUST READINESS ASSESSMENT USING OUR SAAS PLATFORM, MYCSF

Allows you to self-assess using the standard methodology, requirements, and tools provided under the HITRUST Assurance Program.

3

PREPARE FOR A HITRUST VALIDATED ASSESSMENT

Select your authorized HITRUST External Assessor to help with the process. Then utilize MyCSF to streamline preparedness.

4

UNDERGO A HITRUST VALIDATED ASSESSMENT PROCESS USING MYCSF

Our Assurance Team audits your assessment and will issue your certification (with a passing score).

5

RECEIVE YOUR HITRUST LETTER OF CERTIFICATION

For r2 maintain certification every 2 years, complete an r2 Interim Assessment at the 1-year mark. For e1 and i1 maintain certification annually.

HITRUST

Justification for Assurance Investment

46% of breached organizations suffered damage to their reputations and brand value[1]	**75%** of Fortune 20 Companies utilize the HITRUST CSF[2]	**80%** of top cloud service providers use the HITRUST CSF
$3.92 MILLION average cost of a data breach[3]	**60-85%** of controls may be inheritable from Cloud Service Providers[4]	Save on **CYBERSECURITY INSURANCE** premiums with HITRUST Certification
86% of people are unlikely to do business with an organization that suffered a data breach involving card data[5]	**66%** of organizations were hit by ransomware last year[6]	**Save TIME and MONEY** spent on answering questionnaires, with our *Assess Once, Report Many*™ methodology

Data Sources:

[1]Forbes Institute Report
[2]HITRUST Internal Data based on subscription customers and organizations that have downloaded the HITRUST CSF Framework
[3]IBM Security
[4]HITRUST Internal Data (varies by assessment)
[5]Ponemon Institute Report, The Aftermath of a Data Breach: Consumer Sentiment
[6]The State of Ransomware, Sophos

HITRUST®

The HITRUST Approach is Built on a Comprehensive Framework and Robust Assurance Program Designed to Deliver Reliable Assessment Results

REQUIREMENT	APPROACH*					
	HITRUST CSF	ISO 27001	NIST 800-53	PCI SSC DSS	NIST Cybersecurity Framework†	HHS HIPAA‡
Comprehensive Coverage	YES	YES	YES	YES	YES	PARTIAL
Prescriptive Controls	YES	PARTIAL	YES	YES	NO	NO
Practical Controls	YES	YES	NO	YES	YES	YES
Scalable Implementation	YES	YES	NO	PARTIAL	YES	YES
Transparent Update Processes	YES	PARTIAL	YES	NO	YES	NO
Transparent Evaluation & Scoring Methodology	YES	PARTIAL	PARTIAL	PARTIAL	NO	NO
Consistent Results	YES	PARTIAL	YES	PARTIAL	NO	NO
Accurate Results	YES	PARTIAL	PARTIAL	PARTIAL	NO	NO
Efficient Assessment (Assess Once, Report Many)	YES	PARTIAL	PARTIAL	NO	PARTIAL	NO
Reliable Results (Rely-ability)	YES	PARTIAL	PARTIAL	PARTIAL	NO	NO
Certifiable Implementing Entities	YES	YES	PARTIAL	YES	PARTIAL	NO

*Since HITRUST, ISO, NIST and PCI are all RMFs, the document specifying their associated controls is used in the table to uniquely identify them.
†The NIST Cybersecurity Framework is a high-level framework that relies on the specification or design of additional controls to support the framework's recommended outcomes.
‡HIPAA specifies information security requirements (generally at a high level) but is a U.S. federal regulation and not a risk management framework.

HITRUST®

Third-Party Risk Management (TPRM)

The HITRUST Approach can extend beyond your own cybersecurity maturity program to help measure and evaluate the information security strength of business partners with whom you share online networks or sensitive data.

✓ Choose the right HITRUST Assessment to request from vendors based on their level of inherent risk.

✓ Three HITRUST Certification options balance the demands on third-party resources and budgets with the level of assurance needed.

✓ HITRUST Assessments add the confidence your stakeholders need to efficiently vet, assess, and mitigate third party risk.

✓ HITRUST is a trusted, experienced, and innovative resource your organization can count on to assist with Third-Party Risk Management success.

Why Measuring and Managing Third-Party Risk is so Important:

"More than half of organizations have experienced a data breach caused by third parties that led to the misuse of sensitive or confidential information."

Source: "A Crisis in Third-Party Remote Access Security" report conducted by Ponemon Institute

HITRUST®

The HITRUST Results Distribution System (RDS) Simplifies Obtaining, Interpreting, and Analyzing Third-Party Assessment Results

The HITRUST Approach can extend beyond your own cybersecurity maturity program to help measure and evaluate the information security strength of business partners with whom you share online networks or sensitive data.

✓ Choose the right HITRUST Assessment to request from vendors based on their level of inherent risk.

✓ Three HITRUST Certification options balance the demands on third-party resources and budgets with the level of assurance needed.

✓ HITRUST Assessments add the confidence your stakeholders need to efficiently vet, assess, and mitigate third party risk.

✓ HITRUST is a trusted, experienced, and innovative resource your organization can count on to assist with Third-Party Risk Management success.

HITRUST®

Ready to Elevate your Organization's Security and Privacy Posture?

CALL US DIRECTLY
1-855-HITRUST

EMAIL OUR PRODUCT SPECIALISTS
info@HITRUSTAlliance.net

VIEW MORE RESOURCES
HITRUSTAlliance.net