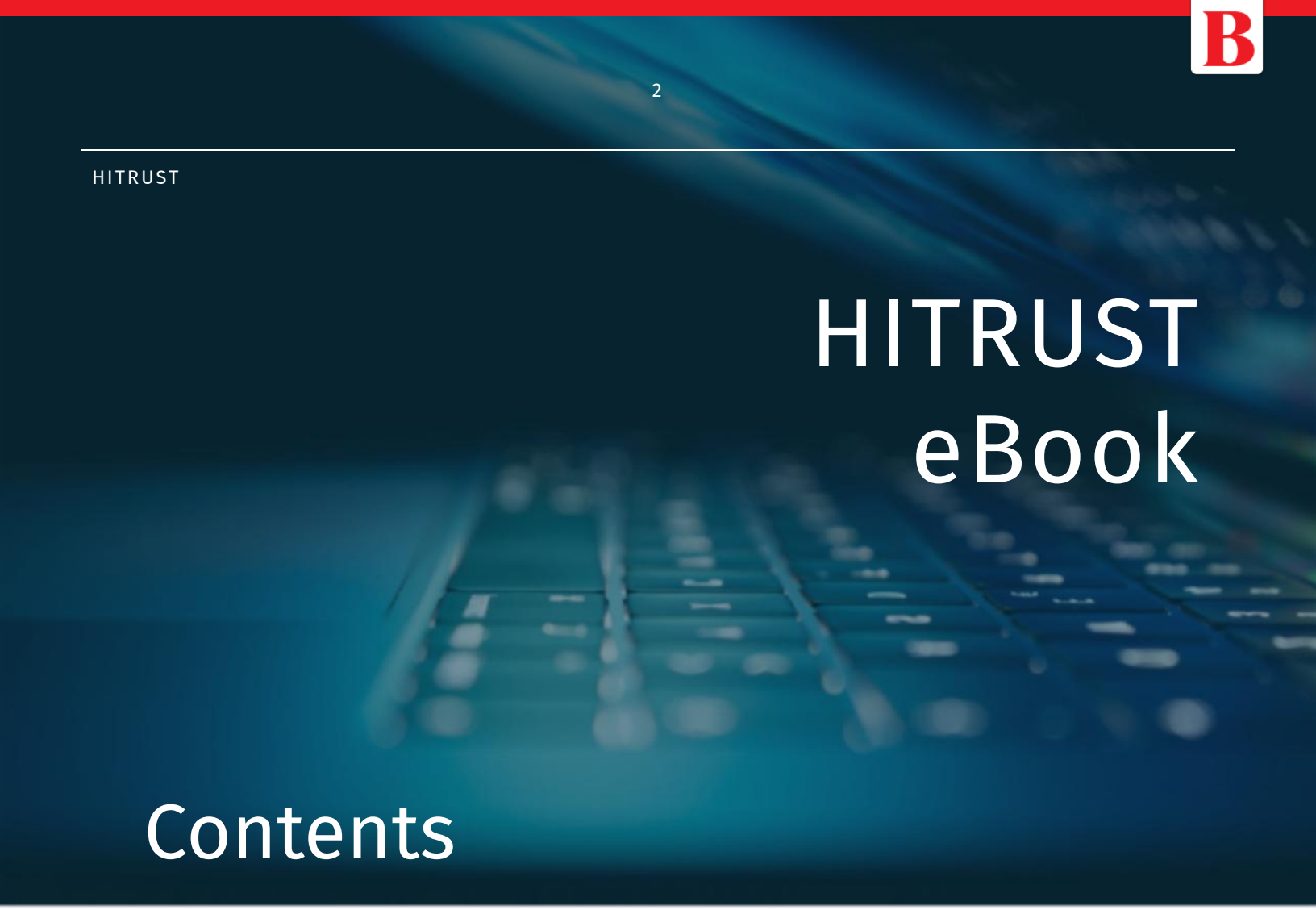
BIG LANGUAGE SOLUTIONS

BIGLanguage.com
+1 404.500.4251
info@biglanguage.com

Understanding the Future of Data Security

A brief history of the HITRUST framework and how it will define data security across multiple industries



HITRUST eBook

Contents

WHAT IS HITRUST?

"HITRUST is a cybersecurity framework created in collaboration with healthcare, technology organizations, and information security organizations, specifically designed to help organizations manage data, information, risk, and compliance."

History

HITRUST is a cybersecurity framework created in collaboration with healthcare, technology organizations, and information security organizations, specifically designed to help organizations manage data, information, risk, and compliance.

Founded in 2007, HITRUST originally stood for the Health Information Trust Alliance, but was subsequently rebranded to HITRUST Alliance. The rebrand to HITRUST Alliance evolved as the framework changed to include regulations, best practices, and frameworks that applied to multiple industries, moving away from a strict healthcare focus to a broader, more industry-agnostic approach.

It was initially aimed at the healthcare sector by providing a robust, certifiable framework for healthcare organizations and their business partners to consistently and efficiently demonstrate their commitment to security and compliance.

As the certification's reputation grew and was widely acknowledged as the most comprehensive security framework, it has become increasingly popular in other sectors.

HITRUST APPROACH

The HITRUST approach Is a multi-pronged program that guides organizations to effectively manage data, information risk, and compliance in a complex and ever-changing environment.

Traditionally, when an organization is developing an information risk and compliance program, they have a bewildering array of considerations:

- Sharing control responsibilities with service providers
- Integrating information risk and compliance controls into an assessment tool
- Measuring the effectiveness of implementation

HITRUST's understanding of information risk management, compliance, and the challenges of assembling and maintaining various programs has resulted in an integrated approach with the various elements aligned, maintained, and comprehensive to support an organization's risk management and compliance.

The components of the HITRUST approach include:

- HITRUST CSF - privacy and security controls framework
- HITRUST Threat Catalogue - anticipated threats mapped to specific CSF controls
- HITRUST MyCSF - a management platform for assessment and corrective action
- HITRUST Assessment XChange - automated sharing of assurances between organizations
- HITRUST CSF Assurance Program - provide assurances to stakeholders
- HITRUST Shared Responsibility Program - customer and cloud service provider requirements
- HITRUST Third Party Assurance Program - third party risk management

The HITRUST Approach removes the need for an organization to subject itself to multiple assessments and reports. It is based on the most up-to-date framework and incorporates international, federal, state regulations regarding security and privacy.

Leading the market, HITRUST integrates with 40+ authoritative sources from HIPAA to ISO and NIST to EU GDPR and is seen as the gold standard in risk management frameworks.

HITRUST CSF

The HITRUST Common Security Framework (CSF) Certification is recognized globally and demonstrates an organization's compliance with rigorous and comprehensive security and privacy protection requirements laid out in the HITRUST CSF.

Achieving certification shows that an organization adheres to information security standards and is proactive in its approach to data protection and risk mitigation. To gain certification, an organization will need to be externally assessed; HITRUST's quality assurance team will check this assessment for quality and consistency, review all controls, documentation, policies, and more.

> *"Achieving certification shows that an organization adheres to information security standards(...)"*

Why is HITRUST CSF Certification Important?

HITRUST CSF Certification has become the benchmark for data protection standards in numerous industries, from the financial sector to language services companies. It is more widely adopted in industries that handle sensitive data, helping organizations, business associates, and downstream suppliers manage IT risk and compliance with IT security regulations.

Achieving HITRUST CSF Certification indicates that information security and privacy are a priority for an organization and prove to its business associates and partners that it meets the certification framework's high-security standards.

Organizations that have achieved the rigorous standards required for certification comprise an elite group of businesses who can reassure their partners that they are obsessive about compliance, and up-to-date with industry-specific regulations, including over forty other frameworks that an organization may be obligated to consider when choosing companies to work with.

BENEFITS OF BECOMING HITRUST CSF CERTIFIED

For businesses in every sector, being HITRUST CSF certified tells their customers that they can have confidence in them and their ability to manage data securely. This credibility level can make the difference between getting the contract or being left out in the cold.

Consider this: according to IBM security, the average cost of a data breach is $3.92 million, and 46% of breached organizations suffer damage to brand value and reputation. Working with a HITRUST CSF Certified business reduces an organization's cyber risk today and into the future.

Additionally, in a Ponemon Institute Report, "The Aftermath of a Data Breach: Consumer Sentiment, 86% of companies were unlikely to do business with an organization that suffered a data breach involving card data.

80% of the top cloud service providers use HITRUST CSF, as do 75% of the Fortune 20 companies. HITRUST CSF Certification can save you money by reducing the amount you pay for cybersecurity insurance from a cost perspective.

HITRUST has several positive comments from leading industry businesses to highlight the competitive advantage of being certified offers. Here are a few for illustrative purposes; you can find more **here**.

> *'You get the credibility, we improved our business processes and were able to reduce our cybersecurity insurance costs'*
> CFO & COO, technology service organization, New Jersey.

> *'Our company recouped our investment in getting certified within 30 days.'*
> CEO, healthcare IT startup, California.

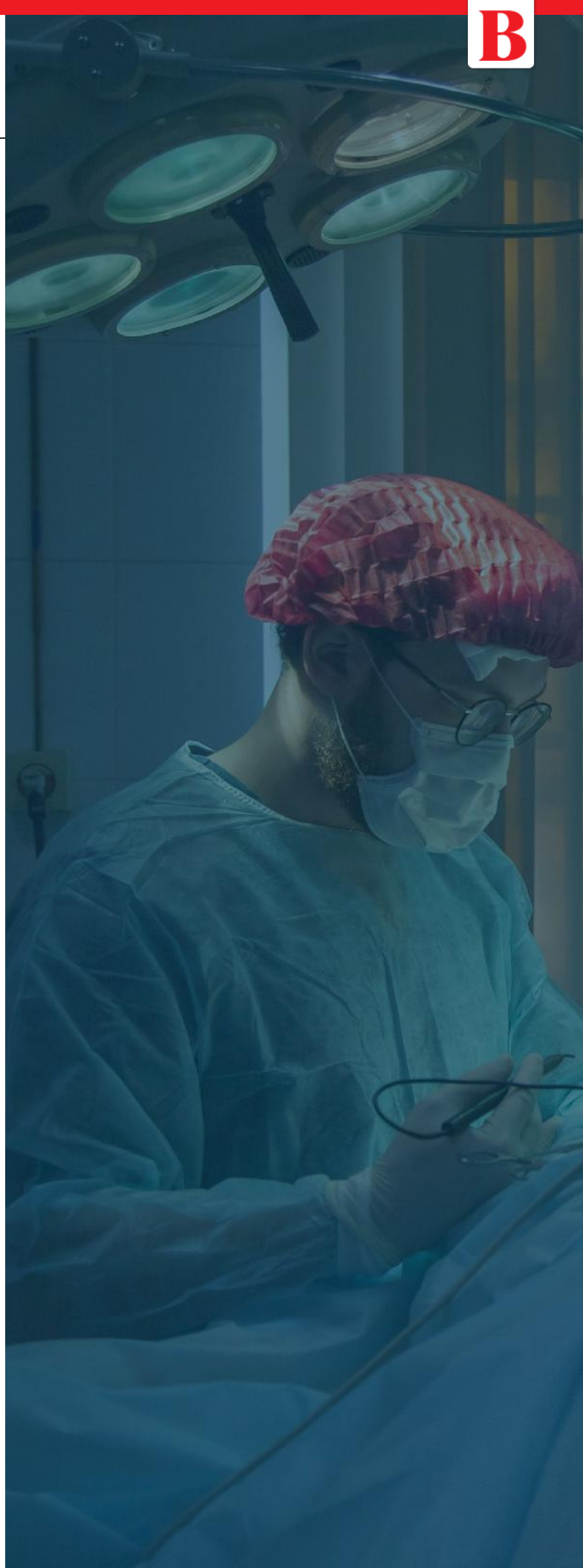
> *'Approximately 40-50% of the prior year's revenue was due to our organization's HITRUST CSF Certification.'*
> CISO, technology organization, Wisconsin. (Source)

The majority of US Healthcare providers view the HITRUST CSF control framework as extremely beneficial. 81% of hospitals and 83% of US Health plans utilize HITRUST CSF. In a 2018 survey by the Healthcare Information Management Systems Society (HIMSS), HITRUST CSF was the most popular and trusted control framework in the healthcare industry.
For assessing third-party risk, the HITRUST CSF Assurance program is the most widely adopted.

> *"81% of hospitals and 83% of US Health plans utilize HITRUST CSF."*

A final benefit of HITRUST CSF certification is that it fully incorporates other common risk management frameworks. The National Industry of Technology and Standards (NIST) is used primarily by US Federal Agencies and the public and private sector, and the Organisation for International Standards (ISO), which non-US organizations use.

There is no need to certify separately for these and over forty other frameworks, including HIPAA, if you opt for HITRUST CSF Certification.



HITRUST SHARED RESPONSIBILITY PROGRAM

The HITRUST Shared Responsibility program looks at the challenges businesses face when dealing with their cloud service providers. The HITRUST Shared Responsibility Model (SRM) is the industry's first commonly accepted model for sharing responsibility in the cloud.

Organizations benefit from this model by ensuring that cloud service providers communicate appropriate security and privacy assurances, get better guidance on the delineation of control ownership, and simplify customer assurance processes.

The shared responsibility matrix is designed to allow customers to discuss cloud supply chain risk. It has an out-of-the-box template, pre-populated with shared responsibility for the cloud, includes over 2000 detailed security and privacy control requirements.

As a result, leading cloud service providers have partnered with HITRUST to publish Shared Responsibility matrices jointly. Cloud service providers we have partnered with include Amazon Web Services, Google Cloud, and Microsoft Azure, among others.

HITRUST THREAT CATALOGUE

The threat catalog was developed over many years by HITRUST to identify a complete set of threats.

As Dr. Bryan Cline explains, *'...a comprehensive threat list that could support risk analysis and help organizations better understand and mitigate threats to sensitive information was essentially unavailable.'*

It maps the threats to controls in the HITRUST CSF Framework, allowing organizations to identify sensitive information, assets, and operational threats.

Additionally, the catalog also maps threats to less comprehensive threat lists from other frameworks, including the National Institute of Standards and Technology (NIST) and the European Network and Information Security Agency Threat Taxonomy (ENISA). The threat catalog will be part of the HITRUST CSF v10 release.

WHAT IS THE FUTURE FOR HITRUST?

HITRUST's background was firmly rooted in the US healthcare space, but companies in other sectors indicate that they are gaining a competitive edge by achieving HITRUST CSF certification.

Other industries, including financial services and other service-based industries - for example, language service companies - that exchange sensitive data, have benefited from HITRUST Certification and have moved to HITRUST because its overarching framework and authoritative sources are increasingly industry agnostic.

The release of HITRUST CSF v10 in 2021 will continue to be increasingly industry agnostic and provide for the needs of the travel, tourism, and financial services sectors to support its continued expansion outside of the healthcare industry.

> *"Other industries, including financial services and other service-based industries, that exchange sensitive data, have benefited from HITRUST Certification(...)"*

GLOBAL EXPANSION

The HITRUST CSF has plans to expand into overseas markets, with an exploratory toe into the Asia Pacific region. This is part of a global information protection goal for information risk management and compliance for businesses of any type, size, or geography. They plan to deliver services locally, nationally, and internationally.

This builds on the HITRUST Approach and their vision of One Framework, One Assessment, Globally.

To facilitate their goal of expanding internationally, they have embarked upon several focus projects, including:

- Establishing an Asia advisory council and appealed for nominations from suitably qualified applicants. Extensive experience in risk management, privacy, and security are prerequisites. An understanding of security and privacy laws relevant to Asian businesses is essential. The Asia Advisory Council ensures the HITRUST Approach remains relevant to the needs of Asia Pacific communities. The Asia Advisory Council's key role is to work with HITRUST to ensure the HITRUST Approach sets the bar for companies in the region to achieve comprehensive, tailored privacy and security risk management solutions.

- Updating HITRUST CSF framework with Asia-specific authoritative sources. These updates will be delivered over three phases. Phase 1 will include data privacy regulations for Hong Kong, Malaysia, and the Philippines, incorporating these countries' Acts of Parliament into the authoritative sources. Phase 2 will address banking and financial services regulations, and phase 3 will include cybersecurity and IT regulations.

> *"The HITRUST Approach and their vision of One Framework, One Assessment, Globally."*

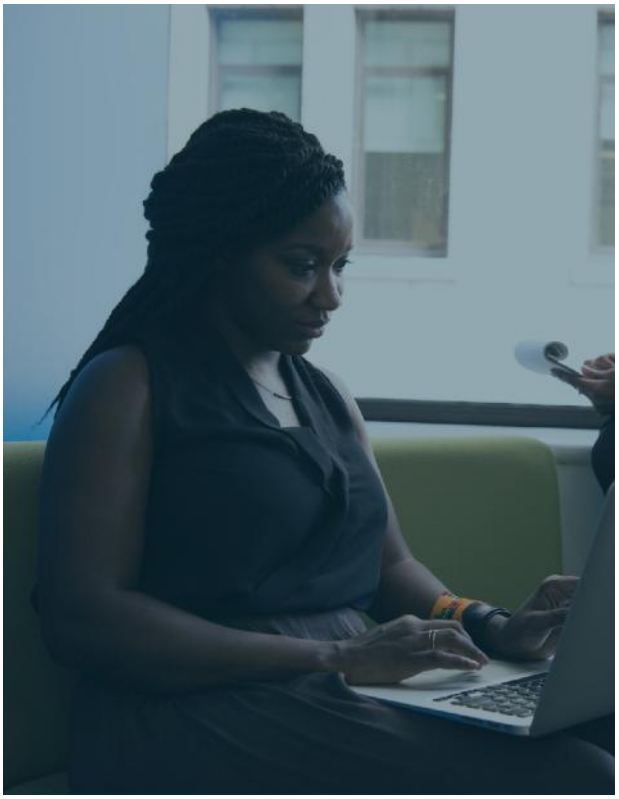
- Supporting data localization in HITRUST CSF, enabling subscribers to specify where the data is held. This ensures they comply with data localization requirements.

- Applying to be an Accountability Agent under the Asia Pacific Economic Cooperation (APEC) Cross Border Privacy Rules System (CBPRS) and Privacy Recognition for Processors System (PRPS).

HITRUST is determined that businesses of all sizes will have access to the most comprehensive, globally relevant information protection framework and services. The HITRUST CSF and CSF Assurance Program offer a single integrated approach to information risk management that can easily be shared with customers and authorities.

UPDATING THE HITRUST PRISMA MATURITY MODEL

The HITRUST approach to evaluate controls differs from the Preferred Reporting Items for Systemic Review and MetaAnalyses (PRISMA) in that it isn't binary and doesn't focus on operational effectiveness and design.



The HITRUST five-point maturity model, which are evaluated against is as follows:

1. **Policy** - Are company expectations clear in written policies? Are they approved and have they been communicated to appropriate personnel?
2. **Procedure** - Are operational aspects of the control defined, approved, and communicated clearly?
3. **Implementation** - Are the controls in place and performing as expected?
4. **Measured** - Can the organization see if a control isn't working?
5. **Managed** - Is the organization responding to risks and addressing them?

The updated PRISMA model that assessors now evaluate against has changed, giving the greatest weighting to implementation. All other aspects of the Maturity Model have little relevance unless everything is being implemented effectively.

So, what does this mean for organizations going for HITRUST CSF Certification?
The shift in the weighting of the maturity model's various elements shows an increasing emphasis on cybersecurity, a direct reflection of the rapidly changing world around us.
HITRUST's message from these PRISMA weighting updates is unambiguous: having well-documented policies and procedures is not enough; effective implementation of internal controls is essential to HITRUST CSF certification.

SUMMARY

HITRUST's position as a dominant force in US healthcare risk management certi fication is firmly established. Its growing adoption by other sectors is evidence of its excellent reputation and rigorous certi fication requirements.

The HITRUST framework incorporates so many other regulatory risk management organizations that are prevalent in both the public and private sectors. Government and federal agencies can only help make it the certification of choice for an increasing number of non-healthcare organizations.

The wide range of resources available to companies looking to certify is impressive and gives organizations everything they need to evaluate and implement what is required to achieve certi fication successfully.

HITRUST's global expansion plans, initially into Asia, built on the HITRUST Approach and their vision of *One Framework, One Assessment, Globally* looks like it may only be the start. It will be of interest to other regions of the world if their Asia expansion is successful, as they continue to push the boundaries of risk management and data security to other regions.

As a HITRUST CSF certified company, ISI Language Solutions has close to 40 years of experience delivering industry-specific language access and localization solutions.

As a HITRUST and ISO 9001:2015 certified language solutions specialist, our efficient processes ensure compliance with regulatory requirements for health plans communicating personal health information (PHI) with members and maximize effective understanding in provider/patient communications.

We are the ideal translation and localization specialists to take your brand global and open up new markets around the world.

Contact us at (818) 753-9181 to find out more.