HITRUST®

HITRUST Implemented, 1-year (i1)

Certification Report

Chinstrap Penguin Corp.

Valid for the period
January 6, 2025 - January 6, 2026

SAMPLE FOR ILLUSTRATIVE USE ONLY

Contents

6175 Main Street
Suite 400
Frisco, TX 75034

1. Letter of HITRUST Implemented, 1-year (i1) Certification

January 6, 2025

Chinstrap Penguin Corporation
123 Main Street
Anytown, TX 12345

HITRUST has developed the HITRUST CSF, a certifiable security and privacy framework which incorporates information protection requirements based on input from leading organizations. HITRUST identified a subset of the HITRUST CSF requirements that an organization must meet to be HITRUST Implemented, 1-year (i1) Certified for a defined assessment scope. Chinstrap Penguin Corp. ("the Organization") has chosen to perform a HITRUST CSF v11.3.2 i1 validated assessment utilizing a HITRUST Authorized External Assessor Organization ("External Assessor") and this report contains the results of the assessment.

Scope

The following platforms of the Organization were included within the scope of this assessment ("Scope") which included a review of the referenced facilities and supporting infrastructure for the applicable information protection requirements:

Platform:

- Customer Central residing at Pelican Data Center

Facilities:

- CP Framingham Manufacturing Facility (Other) located in Framingham, Massachusetts, United States of America
- CP Headquarters and Manufacturing (Other) located in Las Vegas, Nevada, United States of America
- Pelican Data Center (Data Center) managed by Pelican Hosting located in Salt Lake City, Utah, United States of America

Certification

The Organization has met the criteria specified as part of the HITRUST Assurance Program to obtain a HITRUST i1 validated assessment report with certification ("Certification") for the Scope. Certification is awarded based on each domain's average maturity score meeting a minimum score. Within each domain the maturity scores for each requirement statement were validated by an External Assessor and the assessment was subjected to quality assurance procedures performed by HITRUST.

The Certification for the Scope is valid for a period of one year from the date of this letter assuming the following occurs. If any of these criteria are not met, HITRUST will perform an investigation to determine ongoing validity of the certification and reserves the right to revoke the Organization's certification.

- No security events resulting in unauthorized access to the assessed environment or data housed therein, including any data security breaches occurring within or affecting the assessed environment reportable to a federal or state agency by law or regulation

- No significant changes in the business or security policies, practices, controls, and processes have occurred that might impact its ability to meet the HITRUST i1 certification criteria specified as part of the HITRUST Assurance Program.

Users of this report can contact HITRUST customer support (*support@hitrustalliance.net)* for questions on using this report.

The Organization's Assertions

Management of the Organization has provided the following assertions to HITRUST:

- The Organization has acknowledged that, as members of management, they are responsible for the information protection controls implemented as required by the HITRUST.

- The Organization has implemented the information protection controls as described within their assessment.

- The Organization maintains the information security management program via monitoring, review, and periodic re-assessments of the information protection controls.

- The Organization has responded honestly, accurately, and completely to inquiries made throughout the assessment process and certification lifecycle.

- The Organization has provided the External Assessor with accurate and complete records and necessary documentation related to the information protection controls included within the scope of its assessment.

- The Organization has disclosed all design and operating deficiencies in its information protection controls of which is it aware throughout the assessment process, including those where it believes the cost of corrective action may exceed the benefits.

- No events or transactions have occurred or are pending that would have an effect on the assessment that was performed and used as a basis by HITRUST for issuing the report.

- There have been no communications from regulatory agencies concerning noncompliance with or deficiencies regarding the information protection controls that are included within the Scope of this assessment.

External Assessor Responsibilities

External Assessors are authorized by HITRUST based upon a thorough vetting process to demonstrate their ability to perform HITRUST CSF assessments, and individual practitioners are required to maintain appropriate credentials based upon their role on HITRUST assessments. In HITRUST i1 validated assessments the External Assessor is responsible for:

- Reviewing and gaining a detailed understanding of the information provided by the Organization.

- Performing sufficient procedures to validate the control maturity scores provided by the Organization.

- Meeting all HITRUST Assessment criteria described within the HITRUST Assessment Handbook.

HITRUST Responsibilities

HITRUST is responsible for maintenance of the HITRUST CSF and HITRUST Assurance Program against which the Organization and an External Assessor completed this assessment.

HITRUST performed a quality assurance review of this assessment to support that the control maturity scores were consistent with the results of testing performed by the External Assessor. HITRUST's quality assurance review incorporated a risk-based approach to substantiate the External Assessor's procedures were performed in accordance with the requirements of the HITRUST Assurance Program.

Additional information on the HITRUST Assurance Program can be found at the HITRUST website (https://hitrustalliance.net).

Limitations of Assurance

The HITRUST Assurance Program is intended to gather and report information in an efficient and effective manner. An organization should use this assessment report as a component of its overall risk management program. The assessment is not a substitute for a comprehensive risk management program but is a critical data point in risk analysis. The assessment should also not be a substitute for management oversight and decision-making but, again, leveraged as a key input.

HITRUST

2. Assessment Context

About the HITRUST i1 Assessment and Certification

The HITRUST i1 assessment is designed to address the need for a continuously-relevant cybersecurity assessment that incorporates best practices and leverages the latest threat intelligence to maintain applicability with information security risks and emerging cyber threats, such as ransomware and phishing. The i1 Assessment is intended for organizations needing a moderate level of assurance against HITRUST CSF framework that delivers full transparency, accuracy, consistency, and integrity.

HITRUST carefully curates the HITRUST CSF requirements in an i1 assessment to consider good security hygiene controls and cybersecurity best-practice controls. This design affords a high degree of coverage against authoritative sources generally viewed as security best practices. As a result, the HITRUST CSF requirements included in i1 Assessments provide a high degree of coverage against sources such as the HIPAA Security Rule; NIST SP 800-171; the NAIC Data Security Law; the FTC's GLBA Safeguards Rule; NISTIR 7621: Small Business Information Security Fundamentals; the DOL's EBSA Cybersecurity Program Best Practices; and the HITRUST CSF requirements included in HITRUST's Essentials, 1-year (e1) assessment.

The i1 was also designed to be an evolving, threat-adaptive assessment and accompanying certification that leverages threat intelligence and best practice controls to deliver an assessment that addresses relevant practices and active cyber threats. In addition, HITRUST continually evaluates cybersecurity controls to identify those relevant to mitigating known risks using cyber threat intelligence data from leading threat intelligence providers. As a result, the i1 includes controls that were selected exclusively to address emerging cyber threats actively being targeted today.

Assessment Approach

An *Authorized HITRUST External Assessor Organization* (the "External Assessor") performed validation procedures to test the implementation and operation of the HITRUST CSF requirements and corresponding evaluative elements included in this assessment for the scope of the assessment. These validation procedures were designed by the External Assessor based upon the assessment's scope in observance of HITRUST's CSF Assurance Program Requirements and consisted of inquiry with key personnel, inspection of evidence (e.g. access lists, logs, configuration, sample items, policies, procedures, diagrams), on-site or virtual observations, (optionally) utilization of the work of others (as described elsewhere in this report), and (optionally) reperformance of controls.

Each requirement in the HITRUST CSF contains one or more evaluative elements. For example, requirement 0322.09u2Organizational.12, which reads "Media is encrypted when onsite unless physical security can be guaranteed, and always when offsite.", contains the following two evaluative elements: "1. The organization restricts the use of writable, removable media in organizational systems" and "2. The organization restricts the use of personally owned, removable media in organizational systems". The implementation and operation of all evaluative elements associated with applicable HITRUST CSF requirements included in the assessment was evaluated by the external assessor in reaching an implementation score.

HITRUST developed a scoring rubric that is used by External Assessors to determine implementation scoring in a consistent and repeatable way by evaluating both implementation strength and implementation coverage, described as follows:

- The HITRUST CSF requirement's implementation strength is evaluated using a 5-point scale (tier 0 through tier 4) by considering the requirement's implementation and operation across the assessment scope, which consists of all organizational and system elements, including the physical facilities and logical systems / platforms, within the defined scope of the assessment.

- The HITRUST CSF requirement's implementation coverage is evaluated using a 5-point scale (very low through very high) by considering the percentage of the requirement's evaluative elements implemented and operating within the scope of the assessment.

The implementation scoring model utilized on i1 assessments incorporates the following scale. The overall score for each HITRUST CSF requirement ranges from 0 to 100 points in quarter increments based directly on the requirement's implementation score.

Implementation Score	Description	Points Awarded
Not compliant-(NC)	Very few if any of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment. Rough numeric equivalent of 0% (point estimate) or 0% to 10% (interval estimate).	0
Somewhat complaint (SC)	Some of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 25% (point estimate) or 11% to 32% (interval estimate).	25
Partially compliant (PC)	About half of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 50% (point estimate) or 33% to 65% (interval estimate).	50

Implementation Score	Description	Points Awarded
Mostly compliant (MC)	Many but not all of the evaluative elements in HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 75% (point estimate) or 66% to 89% (interval estimate).	75
Fully compliant (FC)	Most if not all of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 100% (point estimate) or 90% to 100% (interval estimate).	100

3. Scope of the Assessment

Company Background

Chinstrap Penguin Corp is a manufacturer, retailer and distributor of widgets for use in the care, feeding and housing of all Antarctic Chinstrap Penguins. Chinstrap Penguin Corp was established in 2005 and has grown to one of the largest widget producers in the world and now offers a number of specialized widgets to its customers and third-party distributors. In 2014 Chinstrap Penguin Corp entered the gadget market by acquiring Gadget Group and is now the third largest gadget manufacturer in the United States.

In-scope Platform

The following table describes the platform that was included in the scope of this assessment.

Customer Central (a.k.a. "Portal")	
Description	The Portal is a platform that allows numerous applications and service offerings to be accessed by customers via a single web-based interface via a browser. It does this for numerous customers and allows their customers to obtain information in a single location. Chinstrap Penguin personnel access the Portal through a secure VPN to a bastion host. From the bastion host systems administrators connect via VDI to an administrative console for management of all in-scope applications and supporting infrastructure. The Portal is developed by Chinstrap Penguin personnel. It is built in Java and .Net. The solution leverages VMWare for scalability. The applications/service offerings that make up the Portal are Penguin Nest, Penguin Analytics, and South Pole Benefit Eligibility. • Penguin Nest is an application that delivers content and applications from customer systems via the Portal. The application collects and feeds critical metrics to Penguin Analytics. • Penguin Analytics is an application that delivers reporting and analytics capability to customers. It allows them to develop dashboards and reports and track KPIs with their information that is stored within the Portal. • South Pole Benefits Eligibility allows our customers to provide benefit eligibility information so that users of the system have a single place to go to get the eligibility information from multiple customers. Meta data from the application is fed to Penguin Analytics for further analysis by customers.
Application(s)	Penguin Nest, Penguin Analytics, South Pole Benefits Eligibility
Database Type(s)	Oracle
Operating System(s)	HP-UX

Customer Central (a.k.a. "Portal")	
Residing Facility	Pelican Data Center
Exclusion(s) from scope	Content and applications from customer systems that are delivered via the Portal are outside the scope of this assessment. This includes customers who choose to leverage the embedded credit card processing page, which is offered as an add-on service. The embedded credit processing page is provided and managed by a third-party service provider.

In-scope Facility

The following table presents the facility that was included in the scope of this assessment.

Facility Name	Type of Facility	Third-party Managed?	Third-party Provider	City	State	Country
CP Framingham Manufacturing Facility	Other	No	-	Framingham	Massachusetts	United States of America
CP Headquarters and Manufacturing	Other	No	-	Las Vegas	Nevada	United States of America
Pelican Data Center	Data Center	Yes	Pelican Hosting	Salt Lake City	Utah	United States of America

Services Outsourced

The following table presents the outsourced service relevant to the scope of this assessment. The "Consideration in this Assessment" column of this table specifies the method utilized for each service provider relevant to the scope of this i1 assessment. Organizations undergoing i1 assessments have two options of how to address situations in which a HITRUST CSF requirement is fully or partially performed by a service provider (e.g., by a cloud service provider):

- The Inclusive method, whereby HITRUST CSF requirements performed by the service provider are included within the scope of the assessment and addressed through full or partial inheritance, reliance on third-party assurance reports, and/or direct testing by the

External Assessor, and

- The Exclusive (or Carve-out) method, whereby HITRUST CSF requirements performed by the service provider are excluded from the scope of the assessment and marked N/A with supporting commentary explaining that the HITRUST CSF requirement is fully performed by a party other than the assessed entity (for fully outsourced controls) or through commentary explaining the excluded partial performance of the HITRUST CSF requirement (for partially outsourced controls).

Third-party Provider	Relevant Service(s) Provided	Consideration in this Assessment
Seashore Office Data Storage	Seashore provides backup tape delivery and storage in a secure offsite facility. No unencrypted customer, covered, or otherwise confidential information is stored here.	Included
Pelican Hosting	Pelican Hosting provides a colocation facility where Chinstrap maintains a dedicated cage. Pelican Hosting personnel do not have logical access to any in-scope systems.	Included

4. Use of the Work of Others

For certain portions of the assessment and as allowed by HITRUST's Assurance Program requirements, the External Assessor may have utilized the work of other assessors, auditors, and/or inspectors in lieu of direct testing. All assessment procedures performed by the External Assessor, including those where the External Assessor utilized the work of others, were subject to HITRUST's quality assurance review procedures. The table below details assessments utilized by the External Assessor.

Potential options available for using the work of others allowed by HITRUST's Assurance Program Requirements include the following and are reflected in the "Utilization Approach" column of the below table if leveraged in this assessment:

- Inheritance of results from or reliance on another HITRUST validated assessment,
- Reliance on a recent third-party assurance report, and/or
- Reliance on testing performed by the assessed entity (i.e., by internal assessors).

Assessment Utilized	Assessed Entity	Assessment Type	Report Date(s)	Utilization Approach	Relevant Platforms	Relevant Facilities	Assessment Domains
Penguin Hosting 2024 Validated Assessment	Penguin Hosting	HITRUST Risk-based, 2-year (r2) Assessment	1/1/2023 to 12/31/2025	Reliance	(All in-scope platforms)	Pelican Data Center	(All assessment domains)

5. Summary Assessment Results

An organization must achieve a straight average score of at least 83 for each assessment domain to qualify for HITRUST Implemented, 1-year (i1) certification.

The table below presents the control maturity scoring averages of all assessment domains included in this assessment alongside the domain scoring averages across all i1 validated assessments submitted to HITRUST (labeled as "Avg. HITRUST i1 score").

Assessment domain	Average domain score of this assessment	Certification scoring threshold of 83 achieved?
01 Information Protection Program	100.00 / 100.00 Avg. HITRUST i1 score: 96.58	Yes
02 Endpoint Protection	100.00 / 100.00 Avg. HITRUST i1 score: 97.31	Yes
03 Portable Media Security	100.00 / 100.00 Avg. HITRUST i1 score: 97.51	Yes
04 Mobile Device Security	100.00 / 100.00 Avg. HITRUST i1 score: 95.05	Yes
05 Wireless Security	100.00 / 100.00 Avg. HITRUST i1 score: 98.31	Yes
06 Configuration Management	100.00 / 100.00 Avg. HITRUST i1 score: 97.60	Yes
07 Vulnerability Management	100.00 / 100.00 Avg. HITRUST i1 score: 96.07	Yes
08 Network Protection	100.00 / 100.00 Avg. HITRUST i1 score: 96.86	Yes
09 Transmission Protection	100.00 / 100.00 Avg. HITRUST i1 score: 97.04	Yes
10 Password Management	100.00 / 100.00 Avg. HITRUST i1 score: 94.72	Yes
11 Access Control	100.00 / 100.00 Avg. HITRUST i1 score: 96.79	Yes

Assessment domain	Average domain score of this assessment	Certification scoring threshold of 83 achieved?
12 Audit Logging & Monitoring	100.00 / 100.00 Avg. HITRUST i1 score: 96.28	Yes
13 Education, Training and Awareness	100.00 / 100.00 Avg. HITRUST i1 score: 95.69	Yes
14 Third Party Assurance	100.00 / 100.00 Avg. HITRUST i1 score: 95.21	Yes
15 Incident Management	100.00 / 100.00 Avg. HITRUST i1 score: 97.61	Yes
16 Business Continuity & Disaster Recovery	100.00 / 100.00 Avg. HITRUST i1 score: 96.05	Yes
17 Risk Management	100.00 / 100.00 Avg. HITRUST i1 score: 98.51	Yes
18 Physical & Environmental Security	100.00 / 100.00 Avg. HITRUST i1 score: 97.36	Yes
19 Data Protection & Privacy	100.00 / 100.00 Avg. HITRUST i1 score: 90.46	Yes

6. Results by Control Reference

Each HITRUST CSF requirement is associated with a HITRUST CSF control reference. The following table is a control reference-level summary of the results for this assessment.

The table below presents the control maturity scoring averages of all HITRUST CSF control references included in this assessment alongside the control reference scoring averages across all i1 validated assessments submitted to HITRUST (labeled as "Avg. HITRUST i1 score").

Control reference	Control specification	Requirement statements	Control ref. average maturity score	Control ref. average maturity score of 80 achieved?
00.a Information Security Management Program	An Information Security Management Program (ISMP) shall be defined in terms of the characteristics of the business, and established and managed including monitoring, maintenance and improvement.	1 applicable	100.00 / 100.00 Avg. HITRUST i1 score: 99.68	Yes
01.a Access Control Policy	An access control policy shall be established, documented, and reviewed based on business and security requirements for access.	1 applicable	100.00 / 100.00 Avg. HITRUST i1 score: 99.28	Yes
01.b User Registration	There shall be a formal documented and implemented user registration and de-registration procedure for granting and revoking access.	1 applicable	100.00 / 100.00 Avg. HITRUST i1 score: 95.79	Yes
01.c Privilege Management	The allocation and use of privileges to information systems and services shall be restricted and controlled. Special attention shall be given to the allocation of privileged access rights, which allow users to override system controls.	3 applicable	100.00 / 100.00 Avg. HITRUST i1 score: 96.52	Yes
01.d User Password Management	Passwords shall be controlled through a formal management process.	4 applicable	100.00 / 100.00 Avg. HITRUST i1 score: 94.34	Yes
01.e Review of User Access Rights	All access rights shall be regularly reviewed by management via a formal documented process.	1 applicable	100.00 / 100.00 Avg. HITRUST i1 score: 94.65	Yes

Control reference	Control specification	Requirement statements	Control ref. average maturity score	Control ref. average maturity score of 80 achieved?
01.f Password Use	Users shall be made aware of their responsibilities for maintaining effective access controls and shall be required to follow good security practices in the selection and use of passwords and security of equipment.	1 applicable	100.00 / 100.00 Avg. HITRUST i1 score: 99.10	Yes
01.g Unattended User Equipment	Users shall ensure that unattended equipment has appropriate protection.	1 applicable	100.00 / 100.00 Avg. HITRUST i1 score: 99.35	Yes
01.h Clear Desk and Clear Screen Policy	A clear desk policy for papers and removable storage media and a clear screen policy for information assets shall be adopted.	1 applicable	100.00 / 100.00 Avg. HITRUST i1 score: 76.64	Yes
01.j User Authentication for External Connections	Appropriate authentication methods shall be used to control access by remote users.	N/A: The Org. deemed all HITRUST CSF requirements in this control reference as not applicable to the scope of this assessment.		
01.k Equipment Identification in Networks	Automatic equipment identification shall be used as a means to authenticate connections from specific locations and equipment.	1 applicable	100.00 / 100.00 Avg. HITRUST i1 score: 99.64	Yes
01.l Remote Diagnostic and Configuration Port Protection	Physical and logical access to diagnostic and configuration ports shall be controlled.	1 applicable	100.00 / 100.00 Avg. HITRUST i1 score: 95.40	Yes

Section 6 has been truncated for this sample report.

Appendix A - Corrective Action Plans Identified

HITRUST requires assessed entities to define corrective action plans (CAPs) for all HITRUST CSF requirements meeting the following criteria: the requirement's overall score is less than 100 (fully compliant) and the associated control reference (e.g., 00.a) averages less than 80. This section lists the CAPs needed to obtain or maintain HITRUST Implemented, 1-year (i1) certification.

Requirement	Control Reference	Maturity Score	Corrective Actions (Unvalidated)
BUID: 11.01e1System.2 / CVID: 2366.0 . The organization reviews all accounts (including user, privileged, system, shared, and seeded accounts), and privileges (e.g., user-to-role assignments, user-to-object assignments) periodically (annually at a minimum).	01.e Review of User Access Rights	75.00	*[Status: Started - On Track, Target Date: 1/31/2025]* Management is implementing a semi-automated bi-monthly compliance the review and monitoring process (e. g., access instructions to perform reviews, IPEs, evidence to demonstrate revocations) for access reviews to demonstrate completeness and accuracy with the review perform by the process owner.
BUID: 13998.02e1Organizational.2 / CVID: 2071.0 . The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors) as part of initial training for new users, prior to accessing any system's information.	02.e Information Security Awareness, Education, and Training	75.00	*[Status: Started - On Track, Target Date: 1/31/2025]* Management is implementing a quarterly semi-automate compliance process to validate on-boarding training completion of employees/contractors (inclusive of recognition and reporting of phishing attempts).
BUID: 13.02e1Organizational.6 / CVID: 2316.0 . Dedicated phishing awareness training is developed as part of the organization's onboarding program, is documented and tracked, and includes the recognition and reporting of potential phishing attempts.	02.e Information Security Awareness, Education, and Training	75.00	*[Status: Started - On Track, Target Date: 1/31/2025]* Management is implementing a quarterly semi-automate compliance process to validate on-boarding training completion of employees/contractors (inclusive of recognition and reporting of phishing attempts).

Appendix B - Additional Gaps Identified

Instances in which a HITRUST CSF requirement scores less than "fully compliant" and the associated control reference (e.g., 00.a) averages 80 or more, a gap is identified instead of a CAP. Remediation of the additional gaps identified is not required but is strongly recommended.

None identified

Appendix C - Assessment Results

Below are the assessment results for each HITRUST CSF requirement included in the assessment.

01 Information Protection Program

Related CSF Control	05.a Management Commitment to Information Security
HITRUST CSF Requirement Statement	**BUID: 0117.05a1Organizational.1 / CVID: 0440.0** A senior-level information security official is appointed. The senior-level information security official is responsible for ensuring the organization s information security processes are in place, communicated to all stakeholders, and consider and address organizational requirements.
Implemented Score	100

Related CSF Control	07.b Ownership of Assets
HITRUST CSF Requirement Statement	**BUID: 0183.07b1Organizational.1 / CVID: 0645.0** All information systems are documented. Documentation of all information systems includes a method to determine accurately and readily the: assigned owner of responsibility; owner’s contact information; and purpose (e.g., through labeling, coding, and/or inventory).
Implemented Score	100

Related CSF Control	06.a Identification of Applicable Legislation
HITRUST CSF Requirement Statement	**BUID: 0181.06a1Organizational.12 / CVID: 0543.0** All relevant statutory, regulatory, and contractual requirements, including the specific controls and individual responsibilities to meet these requirements, are explicitly defined and formally documented (e.g., in policies and procedures, as appropriate) for each information system type, and communicated to the user community as necessary through documented security training and awareness programs.
Implemented Score	100

Appendix C has been truncated for this sample report

Appendix D - HITRUST Background

HITRUST Alliance, Inc. was born out of the belief that information security should be a core pillar of, rather than an obstacle to, the broad adoption of information systems and exchanges. HITRUST®, in collaboration with industry, business, technology and information security leaders, established the HITRUST CSF, a certifiable framework that can be used by any and all organizations that create, access, store or exchange personal, sensitive, and/or financial information.

Beyond the establishment of the HITRUST CSF®, HITRUST is also driving the adoption of and widespread confidence in the framework and sound risk management practices through awareness, education, advocacy, and other outreach activities.

An integral component to achieving HITRUST's goal to advance the protection of sensitive information is the establishment of a practical mechanism for validating an organization's compliance with the HITRUST CSF.

The HITRUST CSF is an overarching security framework that incorporates and leverages the existing security requirements placed upon organizations, including international (GDPR, ISO), federal (e.g., FFIEC, HIPAA and HITECH), state, third party (e.g., PCI and COBIT), and other government agencies (e.g., NIST, FTC, and CMS). The HITRUST CSF is already being widely adopted by leading organizations in a variety of industries as their information protection framework.

HITRUST has developed the HITRUST Assurance Program, which encompasses the common requirements, methodology and tools that enable both an organization and its business partners to take a consistent and incremental approach to managing compliance.

The HITRUST Assurance Program is the mechanism that allows organizations and their business partners and vendors to assess and report against multiple sets of requirements. Unlike other programs, the oversight, vetting, and governance provided by HITRUST and the HITRUST Assessor Council affords greater assurances and security across all industries.

For more information about HITRUST, the HITRUST CSF and other HITRUST offerings and programs, visit *https://hitrustalliance.net.*