HITRUST

HITRUST Risk-based, 2-year (r2)

Certification Report

Chinstrap Penguin Corp.

Valid for the period
August 20, 2024 – August 20, 2026

SAMPLE FOR ILLUSTRATIVE USE ONLY

Contents

1. Letter of HITRUST Risk-based, 2-year (r2) Certification

August 20, 2024

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 Risk-based, 2-year (r2) Certified for a defined assessment scope. Chinstrap Penguin, Inc. ("the Organization") has chosen to perform a HITRUST CSF v11.4 r2 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 (a.k.a "Portal") residing at Pelican Data Center

Facilities:

- CP Framingham Manufacturing Facility (Other) managed internally located in Framingham, Massachusetts, United States of America
- CP Headquarters and Manufacturing (Other) managed internally 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 r2 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 two years 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 r2 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 r2 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 r2 Assessment and Certification

The HITRUST r2 assessment provides the highest level of information protection and compliance assurance. It is the most comprehensive and robust HITRUST certification, and can be optionally tailored to include coverage for additional authoritative sources such as HIPAA, the NIST Cybersecurity Framework, and GDPR.

The HITRUST r2 assessment is an evolving, threat-adaptive assessment with an accompanying certification. HITRUST r2 assessments leverage threat intelligence data and best practice controls to deliver an assessment that addresses relevant practices and active cyber threats. To do this, HITRUST continually evaluates cybersecurity controls to identify those relevant to mitigating known risks using cyber threat intelligence data from leading threat intelligence providers. Therefore, the HITRUST r2 includes controls that exclusively address emerging cyber threats actively being targeted today.

Assessment Approach

An *Authorized HITRUST External Assessor Organization* (the "External Assessor") performed validation procedures to measure the control maturity 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.

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

Implementation Score	Description	Points Awarded
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
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

Risk Factors

The assessed entity completed the following tailoring questionnaire to derive this assessment's customized set of HITRUST CSF requirements based on organizational, geographical, technical, and regulatory risk factors.

Assessment Type	
HITRUST Risk-based, 2-year (r2) Security Assessment	
General Risk Factors	
Organization Type	Service Provider (Information Technology, IT)
Entity Type	Healthcare - Business Associate
Do you offer Infrastructure as a Service (IaaS)?	No
Organizational Risk Factors	
Number of Records that are currently held	Between 10 and 60 Million Records

Technical Risk Factors	
Is the system(s) accessible from the Internet?	Yes
Is the scoped system(s) (on-premise or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)?	No – The systems are only accessible by internal resources. Data is not shared and there is no direct third-party access.
Does the system(s) transmit or receive data with a third-party?	No - There are no publicly positioned systems in the environment or on Chinstrap's devices. Data is not shared and there is no third-party access
Is the system(s) publicly positioned?	No - The system is not publicly positioned
Number of interfaces to other systems	25 to 75
Number of users of the system(s)	Fewer than 500
Number of transactions per day	6,750 to 85,000
Does the scoped environment allow dial-up/dial-in capabilities (i.e., functional analog modems)?	No - There are no modems in the solution
Is scoped information sent and/or received via fax machine (i.e., an actual machine, excluding efax or scan to email)?	No - No fax machines used in the environment
Do any of the organization's personnel travel to locations the organization deems to be of significant risk?	No - No Chinstrap personnel travel to locations deemed to be of significant risk.
Are hardware tokens used as an authentication method within the scoped environment?	No - There are no hardware tokens in use.
Does the organization allow personally owned devices to connect to scoped organizational assets (i.e., BYOD - bring your own device)?	Yes
Are wireless access points in place at any of the organization's in-scope facilities?	No - There are no wireless access points in the environment.
Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component?	No - There is no in-house or outsourced information systems development.
Does the organization use any part of the scoped systems, system components, or system services to sell goods and/or services?	Yes
Does the organization allow the use of electronic signatures to provide legally binding consent within the scoped environment, e.g., simple or basic electronic signatures (SES), advanced electronic or digital signature (AES), or qualified advanced electronic or digital signatures (QES)?	No - There are no electronic signatures in use.
Is scoped information sent by the organization using courier services, internal mail services, or external mail services (e.g., USPS)?	Yes

Is any aspect of the scoped environment hosted on the cloud?	No – No aspect of the scoped environment is hosted on the cloud
Does the system allow users to access the scoped environment from an external network that is not controlled by the organization?	Yes
Regulatory Risk Factors (Optional)	
Subject to State of Massachusetts Data Protection Act	
Subject to State of Nevada Security of Personal Information Requirements	

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

Customer Central (a.k.a. "Portal")	
Database Type(s)	Oracle
Operating System(s)	HP-UX
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 Facilities

The following table presents the facilities that were included in the scope of this assessment.

Facility Name	Type of Facility	Third-party Managed?	Third-party Provider	City	State	Country
Pelican Data Center	Data Center	Yes	Pelican Hosting	Salt Lake City	UT	United States of America
CP Headquarters and Manufacturing	Office	No	N/A	Las Vegas	NV	United States of America
CP Framingham Manufacturing Facility	Other	No	N/A	Framingham	MA	United States of America

Services Outsourced

The following table presents outsourced services relevant to the scope of this assessment. The “Consideration in this Assessment” column of the following table specifies the method utilized for each service provider relevant to the scope of this r2 assessment. HITRUST requires that the inclusive method be used on all r2 assessments but allows use of both the inclusive and exclusive methods on HITRUST Implemented, 1-year (i1) validated assessments. Organizations undergoing i1 validated 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 i1 assessment and addressed through full or partial inheritance, reliance on third-party assurance reports, and/or direct testing, and
- The Exclusive (or Carve-out), method, whereby HITRUST CSF requirements performed by the service provider are excluded from the scope of the i1 assessment and marked as N/A with supporting commentary that specifies that the HITRUST CSF requirement is fully performed by a party other than the assessed entity (for fully outsourced controls) or through commentary describing the excluded partial performance of the control (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	Inheritance	Customer Central (a.k.a. "Portal")	Pelican Data Center	11: Access Control, 18: Physical & Environ.

5. Summary Assessment Results

The required controls for HITRUST Risk-based, 2-year (r2) certification identified in the HITRUST CSF reflect the controls needed to mitigate the most common sources of breaches. An organization must achieve a straight average score of at least 62 for each assessment domain to qualify for HITRUST Risk-based, 2-year (r2) 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 r2 submitted to HITRUST (labeled as "Avg. HITRUST r2 score").

Assessment domain	Policy maturity average score in this assessment	Process maturity average score in this assessment	Implemented maturity average score in this assessment	Average domain score of this assessment	Certification scoring threshold of 62 achieved?
01 Information Protection Program	15.00 / 15.00 Points	20.00 / 20.00 Points	40.00 / 40.00 Points	75.00 / 75.00 Avg. HITRUST r2 score: 74.76	Yes
02 Endpoint Protection	15.00 / 15.00 Points	20.00 / 20.00 Points	40.00 / 40.00 Points	75.00 / 75.00 Avg. HITRUST r2 score: 74.85	Yes

Section 5 has been truncated for this sample report.

6. Results by Control Reference

To assist organizations with prioritizing and focusing efforts, HITRUST established a list of the following priority controls based on an analysis of breach data and input obtained from over 100 security professionals. By implementing these controls, organizations mitigate threats and exposures that are most likely to result in a breach. An organization must implement these controls to qualify for HITRUST r2 Certification.

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 r2 submitted to HITRUST (labeled as "Avg. HITRUST r2 score").

Control reference *(* indicates required for r2 cert.)*	Control specification	Requirement statements	Control ref. average maturity score	Control ref. average maturity score of 71 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	75.00 / 75.00 Avg. HITRUST r2 score: 77.90	Yes
01.b User Registration*	There shall be a formal documented and implemented user registration and de-registration procedure for granting and revoking access.	9 applicable	70.56 / 75.00 Avg. HITRUST r2 score: 73.24	No
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.	8 applicable	72.50 / 75.00 Avg. HITRUST r2 score: 72.17	Yes
01.d User Password Management*	Passwords shall be controlled through a formal management process.	12 applicable	75.00 / 75.00 Avg. HITRUST r2 score: 71.57	Yes
01.e Review of User Access Rights*	All access rights shall be regularly reviewed by management via a formal documented process.	3 applicable	68.33 / 75.00 Avg. HITRUST r2 score: 73.35	No
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	75.00 / 75.00 Avg. HITRUST r2 score: 72.55	Yes

Control reference *(* indicates required for r2 cert.)*	Control specification	Requirement statements	Control ref. average maturity score	Control ref. average maturity score of 71 achieved?
01.j User Authentication for External Connections*	Appropriate authentication methods shall be used to control access by remote users.	3 applicable	75.00 / 75.00 Avg. HITRUST r2 score: 75.99	Yes
01.l Remote Diagnostic and Configuration Port Protection*	Physical and logical access to diagnostic and configuration ports shall be controlled.	1 applicable	75.00 / 75.00 Avg. HITRUST r2 score: 73.07	Yes
01.m Segregation in Networks*	Groups of information services, users, and information systems should be segregated on networks.	1 applicable	75.00 / 75.00 Avg. HITRUST r2 score: 74.64	Yes
01.n Network Connection Control*	For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications.	1 applicable	75.00 / 75.00 Avg. HITRUST r2 score: 74.94	Yes
01.o Network Routing Control*	Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.	1 applicable	75.00 / 75.00 Avg. HITRUST r2 score: 74.70	Yes
01.q User Identification and Authentication*	All users shall have a unique identifier (user ID) for their personal use only, and an authentication technique shall be implemented to substantiate the claimed identity of a user.	9 applicable	68.33 / 75.00 Avg. HITRUST r2 score: 73.40	No

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 71, the requirement's implemented maturity level scores less than "fully compliant", the associated control reference (e.g., 00.a) is required for HITRUST Risk-based, 2-year (r2) certification, and the associated control reference averages less than 71. This section lists the CAPs needed to obtain and maintain HITRUST Risk-based, 2-year (r2) certification.

Requirement	Control Reference	Maturity Score	Maturity Level(s) Deficient	Corrective Actions (Unvalidated)
BUID: 1166.01e2System.3 / CVID: 0100.0 . User access rights are reviewed after promotions, demotions, and termination of employment or other arrangement with a workforce member ends. User access rights are reviewed and re-allocated when moving from one employment or workforce member arrangement to another within the same organization (i.e., transfer).	01.e Review of User Access Rights	65.00	Implementation	*[Status: Started - On Track, Target Date: 12/31/2024]* The organization will ensure that access rights are reviewed after promotions and demotions.

Appendix B. Additional Gaps Identified

Instances in which a HITRUST CSF requirement scores less than 71 but one or more of the CAP criteria (discussed in this report's prior Appendix) are not met are identified as gaps instead of CAPs. Remediation of these gaps is not required but is strongly recommended. The additional gaps identified in this assessment are as follows:

Requirement	Control Reference	Maturity Score	Maturity Level(s) Deficient
BUID: 1147.01c2System.456 / CVID: 0039.0 . Elevated privileges are assigned to a different user ID from those used for normal business use, all users access privileged services in a single role, and such privileged access is minimized.	01.c Privilege Management	55.00	Implementation

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 and is responsible for ensuring security processes are in place, communicated to all stakeholders, and consider and address organizational requirements.		
Maturity Assessment	Policy 5. Fully Compliant (100%)	Process 5. Fully Compliant (100%)	Implemented 5. Fully Compliant (100%)

Related CSF Control	05.h Independent Review of Information Security		
HITRUST CSF Requirement Statement	**BUID: 0177.05h1Organizational.12 / CVID: 0495.0** . An independent review of the organization's information security management program is initiated by management to ensure the continuing suitability, adequacy, and effectiveness of the organization's approach to managing information security.		
Maturity Assessment	Policy 5. Fully Compliant (100%)	Process 5. Fully Compliant (100%)	Implemented 5. Fully Compliant (100%)

Appendix C has been truncated for this sample report.

HITRUST®

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.*