HITRUST

Healthcare and Public Health (HPH) CPGs

Based upon a HITRUST Essentials, 1-year (e1) Validated Assessment

Chinstrap Penguin Corp.

As of December 3, 2025

SAMPLE FOR ILLUSTRATIVE USE ONLY

View this assessment in the
HITRUST Report Center

HITRUST

Contents

HITRUST
6175 Main Street
Suite 400
Frisco, TX 75034

View this assessment in the HITRUST Report Center

Transmittal Letter

December 3, 2025

Chinstrap Penguin Corp.
123 Main Street
Anytown, Texas 12345

Through HITRUST's "Assess Once, Report Many" capability made possible through the HITRUST CSF, HITRUST has prepared this Healthcare and Public Health Sector (HPH) Cybersecurity Performance Goals (CPGs) ("HPH CPGs") Insights Report at the request of Chinstrap Penguin Corp. ("the Organization"). This Insights Report contains detailed information regarding the coverage and maturity of controls supporting the Organization's compliance with HITRUST CSF requirements mapping to HPH CPGs for the scope outlined below, based on a HITRUST Essentials, 1-year (e1) assessment using v11.7.0 of the HITRUST CSF. The Organization can leverage this report to share information regarding their HPH CPGs compliance efforts with internal and external stakeholders.

The full e1 validated assessment report contains detailed information relating to the maturity of information protection controls as defined by the tailoring factors selected by management of the Organization. It includes detailed assessment results, a benchmark report comparing the Organization's results to industry results, and details on corrective action plans (if applicable). Such detailed information can best be leveraged by relying parties who are familiar with and understand the services provided by the Organization. Those interested in obtaining a copy of the full report should contact the Organization directly.

Scope

The e1 assessment that this Insights Report is based upon included the following platform, facilities, and supporting infrastructure of the Organization ("Scope"):

Platform:

- Customer Central (a.k.a. "Portal") residing at Pelican Data Center

Facilities:

- CP Framingham Manufacturing Facility (Office) located in Framingham, MA, United States of America

- Pelican Data Center (Data Center) located in Salt Lake City, UT, United States of America

The Organization's Responsibilities and Assertions

Management of the Organization is responsible for the implementation, operation, and monitoring of the control environment for the Scope. Through execution of this responsibility, and completion of a HITRUST Essentials, 1-year (e1) validated assessment, the Organization asserted that management of the Organization:

- Is responsible for the implementation of information protection controls.
- Disclosed all design and operating deficiencies in their information protection controls which they are aware, including those for which they believe the cost of corrective action may exceed the benefits.
- Is not aware of any events or transactions that have occurred or are pending that would have an effect on the Essentials, 1-year (e1) validated assessment that was performed and used as a basis by HITRUST for issuing that report.
- Is not aware of communications from regulatory agencies concerning noncompliance with or deficiencies regarding the information protection controls that are included within the scope of the Essentials, 1-year (e1) validated assessment.

Management of the Organization is also solely responsible for ensuring the Organization's compliance with any legal and/or regulatory requirements, including HPH CPGs.

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 on their role in HITRUST assessments. In HITRUST validated assessments, the External Assessor is responsible for the following:

- 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's Responsibilities

HITRUST is responsible for maintenance of the HITRUST CSF and HITRUST Assurance Program against which the Organization completed the accompanying Essentials, 1-year (e1) validated assessment. HITRUST is also responsible for producing the mappings from various authoritative sources, including HPH CPGs, to the HITRUST CSF. Additional information about HITRUST's "Assess Once, Report Many" approach and on the HITRUST CSF Assurance Program used to support this compliance assessment can be found on the HITRUST website at https://hitrustalliance.net.

Limitations of Assurance

Parties relying on this report should understand the limitations of assurance specified in the Limitations of Assurance section of this report.

HITRUST

HITRUST

HPH CPGs Scorecard

The tables below provide insights on HPH CPGs compliance for the environment assessed. Each HPH CPGs requirement listed is assigned a compliance score for the implemented control maturity level. The compliance scores are based on the assessment results of the HITRUST CSF requirement(s) as mapped to the HPH CPGs requirement. The measured and managed control maturity levels are not included in this scorecard, as these control maturity levels were not assessed in the underlying HITRUST CSF assessment as a result of the Organization's assessment tailoring. These mappings can be found in Appendix B of this document.

To learn about the HITRUST control maturity evaluation and scoring approach, visit https://hitrustalliance.net/content/uploads/Evaluating-Control-Maturity-Using-the-HITRUST-Approach.pdf.

Scorecard Color Legend

FC	Fully Compliant: The control maturity level's scores across all HITRUST CSF requirements included in the Organization's HITRUST assessment mapped to the HPH CPGs requirement averaged 90 - 100%.

HITRUST

1 - Essential Goals

Reference	Cybersecurity Performance Goal	Implemented Scoring
1.01	Mitigate Known Vulnerabilities - Reduce the likelihood of threat actors exploiting known vulnerabilities to breach organizational networks that are directly accessible from the Internet.	FC
1.02	Email Security - Reduce risk from common email-based threats, such as email spoofing, phishing, and fraud.	FC
1.03	Multifactor Authentication - Add a critical, additional layer of security, where safe and technically capable, to protect assets and accounts directly accessible from the Internet.	FC
1.04	Basic Cybersecurity Training - Ensure organizational users learn and perform more secure behaviors.	FC
1.05	Strong Encryption - Deploy encryption to maintain confidentiality of sensitive data and integrity of Information Technology (IT) and Operational Technology (OT) traffic in motion.	FC
1.06	Revoke Credentials for Departing Workforce Members, Including Employees, Contractors, Affiliates, and Volunteers - Prevent unauthorized access to organizational accounts or resources by former workforce members, including employees, contractors, affiliates, and volunteers by removing access promptly.	FC

This section has been truncated for this sample report

HITRUST

Assessment Context

About the HITRUST e1 Assessment and Certification

HITRUST e1 assessments address the need for a continuously-relevant cybersecurity assessment focusing on foundational cybersecurity controls and mitigations for the most pressing cybersecurity threats. Organizations successfully achieving an e1 certification can reliably demonstrate they meet a bar of essential cybersecurity hygiene.

This assessment is designed for lower assurance scenarios (such as those needing greater assurances than achieved through information security questionnaires or readiness assessments but less so than those achieved through more robust, higher effort assessments). However, an e1 assessment can also serve as a starting point for enterprises that are in the early stages of implementing their information security controls.

To ensure foundational cybersecurity is in place, e1 assessments focuses on a pre-set selection of HITRUST CSF requirements curated by HITRUST. While not a compliance assessment, the subject matter does overlap with authoritative sources sharing similar goals (such as CISA Cyber Essentials, Health Industry Cybersecurity Practices for Small Healthcare Organizations, NIST SP 800-171's "Basic" requirements, and NIST IR 7621: Small Business Information Security Fundamentals).

HITRUST's analysis of cyber threat intelligence data from leading threat intelligence providers when curating the controls considered during e1 assessments, e1 is an evolving, threat-adaptive assessment. HITRUST continually evaluates this data in relation to the controls included in the e1 to ensure that the e1 continues to address the most critical cyber threats (such as ransomware, phishing, brute force, and abuse of valid accounts).

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.

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 e1 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 Compliant (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

HITRUST

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

Customer Central (a.k.a. "Portal")	
	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
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
CP Framingham Manufacturing Facility	Office	No	-	Framingham	MA	United States of America
Pelican Data Center	Data Center	Yes	-	Salt Lake City	UT	United States of America

HITRUST

Services Outsourced

The following table presents outsourced services 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 e1 assessment. Organizations undergoing e1 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
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

HITRUST

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 Use of the Work of Others, 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).

Work of other assessors was not relied upon in the HITRUST CSF assessment underlying this compliance insights report (i.e., no inheritance or third-party reliance was utilized).

HITRUST

Limitations of Assurance

Relying parties should consider the following in its evaluation of the findings in this report:

- This Insights Report provides transparency into the current state of HPH CPGs coverage and control maturity within the scoped environment for the Organization as described in the 'Coverage and Reportability' section above. This Insights Report supports the Organization in communicating the status of controls supporting HPH CPGs compliance and is not a certification of HPH CPGs compliance.

- This Insights Report accompanies a HITRUST CSF e1 Validated assessment. The accompanying e1 Validated assessment was scoped and performed in accordance with the HITRUST Assurance Program requirements designed to measure and report on control maturity for purposes of issuing HITRUST validated assessment reports. Consequently:

    - The nature, timing, and extent of the procedures performed by the HITRUST External Assessor Organization may differ from those performed in an assessment dedicated exclusively to evaluating HPH CPGs compliance and were not designed to specifically detect all instances of HPH CPGs non-compliance.

    - Compliance deficiencies noted in this report, if any, were identified through an evaluation of control maturity of the HITRUST CSF requirements mapping to HPH CPGs included in the Organization's HITRUST validated assessment and not in observance of any other criteria specific to HPH CPGs requirements.

- Mappings produced by HITRUST to authoritative sources are performed utilizing the NIST OLIR Program methodology outlined in NIST Interagency Report 8278 and subjected to HITRUST's internal quality review process.

- No assessment of controls or compliance status provides total assurance or 100% protection against possible control failures and instances of non-compliance. Because of their nature, controls may not prevent, or detect and correct, all errors or omissions relevant to compliance with regulatory statutes.

HITRUST

HPH CPGs Overview

The Healthcare and Public Health Sector Cybersecurity Performance Goals (HPH CPGs) are a set of voluntary cybersecurity performance goals designed specifically for healthcare and public health organizations that were published by the US Department of Health and Human Services (HHS) for the Healthcare and Public Health (HPH) sector.

The HPH CPGs were adapted from the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) Cross-Sector CPGs and were also informed by common industry cybersecurity frameworks, guidelines, best practices, and strategies including Healthcare Industry Cybersecurity Practices (HICP) and National Institute of Standards and Technology (NIST) Cybersecurity Framework. Within the HPH CPGs publication, each CPG is mapped to related HICP sub-practices to help facilitate implementation.

The HPH CPGs are organized into two levels, Essential Goals and Enhanced Goals.

- There are 10 Essential Goals that are meant to help healthcare organizations address common vulnerabilities by setting a floor of safeguards that will better protect them from cyberattacks, improve response when events occur, and minimize residual risk.

- There are 10 Enhanced Goals to encourage healthcare organizations to mature their cybersecurity capabilities and reach the next level of defense needed to protect against additional attack vectors.

HITRUST

HPH CPGs Coverage and Reportability

A HITRUST validated assessment can provide evidence that specific HITRUST CSF control requirements mapping to HPH CPGs requirements have been implemented, how well they have been implemented, and the nature and volume of identified gaps in implementation. The HITRUST CSF, the inherent mappings to HPH CPGs as a supported authoritative source, and HITRUST's comprehensive assurance program are important tools for organizations who aim to comply with the HPH CPGs.

The following factors collectively determine the degree of CMMC Level 1 coverage and reportability in a HITRUST assessment:

- HITRUST's approach to incorporating the HPH CPGs into the HITRUST CSF
- The Organization's assessment type selection, HITRUST CSF version selection, and assessment tailoring

Approach to incorporating CMMC Level 1 into the HITRUST CSF:

The HITRUST CSF provides full coverage for the HPH CPGs by mapping HITRUST requirement statements to all 20 HPH CPGs.

HPH CPGs Categories

The Organization has the option to include the Essential Goals, Enhanced Goals, or both within their assessment.

HPH CPGs Categories selected by the Organization	Essential Goals, Enhanced Goals

Appendix A: HPH CPGs-relevant Observations

During the Essentials, 1-year (e1) validated assessment, no deficiencies were noted during the evaluation of any HITRUST CSF requirements mapping to the considered HPH CPGs requirements.

None identified

HITRUST

Appendix B: Relevant HITRUST Assessment Results and Mappings

Below are the assessment results and control maturity evaluations for each assessed HITRUST CSF requirement mapped to the areas of HPH CPGs considered in the underlying HITRUST CSF assessment, organized by HPH CPGs part.

This section also shows the HITRUST CSF requirements mapped by HITRUST to each considered HPH CPGs requirement. Note that many more mappings exist between HPH CPGs and the HITRUST CSF; this section lists only the mapping subset relevant to the underlying HITRUST assessment as determined through the factors described in the HPH CPGs Coverage and Reportability section of this document.

In addition to HPH CPGs, the HITRUST CSF is mapped to dozens of additional authoritative sources, enabling a wide range of compliance coverage within HITRUST Assessments. Mappings produced by HITRUST are performed utilizing the NIST OLIR Program methodology outlined in NIST Interagency Report 8278. These mappings were created by HITRUST and have undergone HITRUST's internal quality review process consisting of at least five of review before being finalized: automated review, initial mapper review, peer review, management review, and quality assurance review. Questions about these mappings should be routed to HITRUST's Support team.

1 - Essential Goals

HITRUST CSF Requirement	Implemented Score
1.01: Mitigate Known Vulnerabilities Reduce the likelihood of threat actors exploiting known vulnerabilities to breach organizational networks that are directly accessible from the Internet.	
BUID: 04.01x1Organizational.5 / CVID: 2318.0. The organization identifies and encrypts mobile devices and mobile computing platforms that process, store, or transmit sensitive information.	Fully Compliant
BUID: 11183.01c1System.3 / CVID: 1896.0. System administrators only use accounts with privileged access when performing administrative duties and use a separate user account with standard user access rights when performing non-privileged activities (e.g., Internet browsing, email, or similar activities).	Fully Compliant

HITRUST

HITRUST CSF Requirement	Implemented Score
BUID: 0715.10m1Organizational.4 / CVID: 1375.0. Only necessary and secure services, protocols, daemons, etc., required for the function of the system are enabled. Security features are implemented for any required services, protocols or daemons that are considered to be insecure (e.g., use secured technologies such as SSH, S-FTP, TLS v1.2 or later, or IPsec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.).	Fully Compliant
BUID: 0265.09m1Organizational.2 / CVID: 0943.2. The organization applies a default-deny rule that drops all traffic via host-based firewalls or port filtering tools on its endpoints (workstations, servers, etc.), except those services and ports that are explicitly allowed.	Fully Compliant
BUID: 02.09mHICPOrganizational.3 / CVID: 2343.0. The organization uses network access control (NAC) to manage and authenticate IT assets that attempt to connect to the network.	Fully Compliant
BUID: 0778.10m1Organizational.5 / CVID: 1398.0. The organization regularly compares the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.	Fully Compliant

This section has been truncated for this sample report

HITRUST

Appendix C: 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.