



HITRUST Essentials, 1-year (e1)

Certification Report



Chinstrap Penguin Corp.

Valid for the period
November 12, 2025 - November 12, 2026

This report is provided exclusively for internal
business use by Example Org

Downloaded by john.doe@example.com on 10/1/2026

SAMPLE REPORT FOR ILLUSTRATIVE USE ONLY



View this assessment in the
HITRUST Report Center



Contents

1. Letter of HITRUST Essentials, 1-year (e1) Certification	3
2. Assessment Context	7
About the HITRUST e1 Assessment and Certification	7
Assessment Approach	7
3. Scope of the Assessment	9
4. Use of the Work of Others	12
5. Summary Assessment Results	13
6. Results by Control Reference	14
Appendix A - Corrective Action Plans Identified	15
Appendix B - Additional Gaps Identified	17
Appendix C - Assessment Results	18
01 Information Protection Program	18
02 Endpoint Protection	18
Appendix D - HITRUST Background	19

For Internal Use by Example Org



1. Letter of HITRUST Essentials, 1-year (e1) Certification

February 12, 2025

Chinstrap Penguin Corp.
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 Essentials, 1-year (e1) Certified for a defined assessment scope. Chinstrap Penguin Corp. ("the Organization") has chosen to perform a HITRUST CSF v11.4.0 e1 assessment. The assessment was performed utilizing a HITRUST Authorized External Assessor Organization ("External Assessor").

Scope

The following platform of the Organization was 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 (Office) located in Framingham, MA, United States of America
- CP Headquarters and Manufacturing (Office) located in Las Vegas, NV, United States of America
- Pelican Data Center (Data Center) managed by Pelican Hosting located in Salt Lake City, UT, United States of America

Certification

The Organization has met the criteria specified as part of the HITRUST Assurance Program to obtain a HITRUST Essentials, 1-year (e1) 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 certification criteria specified as part of the HITRUST Assurance Program.

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

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 it is 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 e1 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 about the HITRUST CSF and HITRUST Assurance Program used to support this assessment can be found on 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.

Distribution and Use Restriction

This report is provided exclusively for the internal business use of Example Org. Distribution, publication, or disclosure of this report outside of Example Org, in whole or in part, is prohibited. This document contains recipient-specific identifying information and may be monitored for unauthorized distribution.

HITRUST



2. 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

The External Assessor performed validation procedures based upon the scope of the assessment and in observance of the requirements in the HITRUST Assessment Handbook. Validation procedures 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

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	None

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
CP Headquarters and Manufacturing	Office	No	-	Las Vegas	NV	United States of America
Pelican Data Center	Data Center	Yes	Pelican Hosting	Salt Lake City	UT	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 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



4. Use of the Work of Others

For certain portions of the assessment and as allowed by HITRUST's Assurance Program requirements within the Assessment Handbook, 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).

Assessment Utilized	Assessed Entity	Assessment Type	Utilization Approach	Relevant Platforms	Relevant Facilities	Assessment Domains
Pelican Hosting HITRUST r2	Pelican Hosting	HITRUST r2	Inheritance	(All in-scope platforms)	(All in-scope facilities)	(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 Essentials, 1-year (e1) 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 e1 validated assessments submitted to HITRUST (labeled as "Avg. HITRUST e1 score").

Assessment Domain	Average domain score of this assessment	Certification scoring threshold of 83 achieved?
01 Information Protection Program	100.00 / 100.00 points Avg. HITRUST e1 score: 99.85	Yes
02 Endpoint Protection	100.00 / 100.00 points Avg. HITRUST e1 score: 97.85	Yes
03 Portable Media Security	100.00 / 100.00 points Avg. HITRUST e1 score: 99.75	Yes
04 Mobile Device Security	100.00 / 100.00 points Avg. HITRUST e1 score: 99.57	Yes
05 Wireless Security	100.00 / 100.00 points Avg. HITRUST e1 score: 96.71	Yes

This section has been truncated for this sample report



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 e1 validated assessments submitted to HITRUST (labeled as "Avg. HITRUST e1 score").

Control Reference	Control Specification	Requirement Statements	Control ref. average maturity score	Control ref. average maturity score of 80 achieved?
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 e1 score: 97.60	Yes
01.d User Password Management	Passwords shall be controlled through a formal management process.	2 applicable	100.00 / 100.00 Avg. HITRUST e1 score: 99.37	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 e1 score: 97.93	Yes
01.I 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 e1 score: 99.55	Yes
01.m Segregation in Networks	Groups of information services, users, and information systems should be segregated on networks.	1 applicable	75.00 / 100.00 Avg. HITRUST e1 score: 96.71	No, 1 CAP identified

This section 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 Essentials, 1-year (e1) certification.

Requirement	Control Reference	Maturity Score	Corrective Actions (Unvalidated)
BUID: 0805.01m1Organizational.12 / CVID: 0160.0 . Security gateways (e.g., a firewall) are used between the internal network, external networks (Internet and third-party networks), and any demilitarized zone (DMZ). An internal network perimeter is implemented by installing a secure gateway (e.g., a firewall) between two interconnected networks to control access and information flow between the two domains. This gateway is capable of: enforcing security policies, being configured to filter traffic between these domains, and blocking unauthorized access in accordance with the organizations access control policy. Wireless networks are segregated from internal and private networks. The organization requires a firewall between any wireless network and the covered and/or confidential information systems environment.	01.m Segregation in Networks	75.00	The organization will provide evidence that security gateways are used between the internal network, external networks (Internet and third-party networks), and any demilitarized zone (DMZ). [Status: In progress, Target Date: 2025-04-01]



BUID: 1223.09ac1System.1 / CVID: 1203.1 . Access to audit trails / logs is safeguarded from unauthorized access and use.	09.ac Protection of Log Information	75.00	The organization will review access to audit logs to ensure that access is limited. [Status: In progress, Target Date: 2025-07-15]
---	--	-------	--

For Internal Use by Example Org



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

For Internal Use by Example Org



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	04.a Information Security Policy Document
HITRUST CSF Requirement Statement	BUID: 0113.04a1Organizational.2 CVID: 0431.1 . The organization's information security policy is developed, published, disseminated, and implemented. The information security policy documents: state the purpose and scope of the policy; communicate management's commitment; describe management and workforce members' roles and responsibilities; and establish the organization's approach to managing information security.
Implemented Score	100

02 Endpoint Protection

Related CSF Control	09.m Network Controls
HITRUST CSF Requirement Statement	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.
Implemented Score	100

Related CSF Control	09.k Controls Against Mobile Code
HITRUST CSF Requirement Statement	BUID: 0226.09k1Organizational.2 CVID: 0896.0 . The organization implements and regularly updates mobile code protection, including anti-virus and anti-spyware.
Implemented Score	100

This section 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>.