HITRUST

HITRUST AI Security, 1-year (ai1)

Certification Report

Chinstrap Penguin Corporation

Valid for the period
January 15, 2025 - January 15, 2026

SAMPLE FOR ILLUSTRATIVE USE ONLY

HITRUST

Contents

Several sections have been trucated in this sample report

1. Letter of HITRUST AI Security, 1-year (ai1) Certification Letter

January 15, 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 AI Security, 1-year (ai1) Certified for a defined assessment scope. Chinstrap Penguin Corporation ("the Organization") has chosen to perform the HITRUST AI Security, 1-year (ai1) Validated Assessment utilizing a HITRUST Authorized External Assessor Organization ("External Assessor") and this report contains the results of the assessment.

Scope

The following platforms and the underlying AI models 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 AI Security, 1-year (ai1) Validated Assessment Report with Certification ("Certification") for the Scope. Certification is awarded based upon achieving two criteria. First,

the Organization obtained a HITRUST Essentials, 1-year (e1) Certification which demonstrates that foundational cybersecurity was in place for the Scope. Second, meeting the minimum scoring threshold for requirement statements specific to the HITRUST AI Security, 1-year (ai1) Certification. 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, and

- No significant changes in the business or security policies, practices, controls, and processes have occurred that might impact its ability to meet the HITRUST AI Security 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 AI Security 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.

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 AI risk management program. The assessment is not a substitute for a comprehensive AI risk management program but is a critical data point in AI security risk analysis. The assessment should also not be a substitute for management oversight and decision-making but, again,

leveraged as a key input. Further, this assessment focuses on a very important aspect of AI risk (security) but was not designed to evaluate all aspects of AI risk that an organization may face.

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

HITRUST

2. Assessment Context

About the HITRUST AI Security Assessment and Certification

The HITRUST AI Security Assessment is designed to address the need for a cybersecurity assessment for deployed AI systems. While AI presents opportunities, it also introduces unique risks and compliance challenges that demand attention. Managing the security risks of AI systems is critical, as failing to do so can have severe consequences. The AI Security Assessment is intended for AI providers, including:

- AI *platform* providers: Provides services that enable other organization to deliver AI-enabled products or services.
- AI *product* providers: Provides AI-enabled products directly usable by end-user / end-customer. Also referred to as *AI application providers* throughout this document.

To address the cybersecurity of AI systems, organizations must (1) extend existing IT security practices and (2) proactively address AI security specificities through new IT security practices. The HITRUST AI Security Assessment and Certification equips organizations to do this effectively through providing prescriptive and relevant AI security controls, a means to assess those controls, and reliable reporting that can be shared with internal and external stakeholders.

HITRUST carefully crafted the HITRUST CSF AI security requirement statements by understanding the AI security threat landscape using the HITRUST Threat Catalog as well as AI threat taxonomies, including NIST AI 100-2 and MITRE Atlas; harmonizing almost 2 dozen AI security sources to understand the consensus of the critical AI security controls; and considering inputs from HITRUST's AI working groups and interviews with AI thought leaders.

This *HITRUST AI Security Assessment and Certification* focuses on mitigating the AI security threats that make up the cybersecurity risk that accompanies the deployment of AI within an organization. Cybersecurity risk is one of many risks discussed in AI risk management frameworks like the NIST AI RMF and ISO/IEC 23894:2023. AI risks that are peers to cybersecurity, including those dealing with AI ethics (such as fairness and avoidance of detrimental bias), AI privacy (such as consent for using data to train AI models), and AI safety (i.e., ensuring the AI system does not harm individuals) are not assessed through this assessment.

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 Assessment

Handbook 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 in Section 5 of this report), and (optionally) reperformance of controls.

Each requirement statement in the HITRUST CSF contains one or more evaluative elements. The External Assessor evaluated the implementation and operation of all evaluative elements associated with applicable HITRUST CSF requirements included in the assessment to reach an implementation score.

HITRUST developed a scoring rubric that external assessors use 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 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 AI Security requirements based on their deployed AI system.

What type of AI model(s) are used by in-scope IT platforms?	Generative AI model
Was covered and/or confidential data used to train the model, tune the model, or enhance the model's prompts via RAG?	Yes
Is the model's parameters and technical architecture confidential to the organization?	No

HITRUST

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 customer

Application(s)	Penguin Nest, Penguin Analytics, South Pole Benefits Eligibility
Database Type(s)	Oracle
Operating System(s)	HP-UX
Residing Facilities	Pelican Data Center

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 this table specifies the method utilized for each service provider relevant to the scope of this ai1 assessment. Organizations undergoing ai1

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 Penguin maintains a dedicated cage. Pelican Hosting personnel do not have logical access to any in-scope systems	Included

HITRUST

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 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).

Third-party Report Type	Assessed Entity	Assessment Type	Utilization Approach	Relevant Platforms	Relevant Facilities	Assessment Domains
Pelican Hosting SOC2 Type II	Pelican Hosting	Period-of-Time assessment report (e.g. SOC2 Type II)	Issuance Date: 05/27/2021	Customer Central (a.k.a. “Portal”)	Pelican Data Center	18 Physical & Environmental Security

HITRUST

5. Summary Assessment Results

An organization must achieve a straight average score of at least 83 for each assessment domain to qualify for HITRUST AI Security1-year (ai1) certification and may score up to the maximum score of 100 points. The assessed entity chose to exclude the measured and managed maturity levels from this assessment's scope, making 75 the highest maturity score directly achievable.

The table below presents this assessment's domain averages alongside the average domain scores of from all HITRUST AI Security, 1-year (ai1) Validated Assessments submitted to HITRUST.

Assessment domain	Average domain score of this assessment	Certification scoring threshold of 83 achieved?
01 Information Protection Program	100.00 / 100.00 Avg. HITRUST e1 score: 96.58	Yes
06 Configuration Management	100.00 / 100.00 Avg. HITRUST e1 score: 97.60	Yes

Section 5 has been truncated for this sample report.

HITRUST

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 the AI Security-related control references assessment.

The table below presents the control maturity scoring averages of the AI Security-related 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	AI Security Requirement Statements	Control ref. average maturity score of AI Security requirement statements	Control ref. average maturity score of 80 achieved for AI security requirement statements?
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 e1 score: 99.68	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.	1 applicable	100.00 / 100.00 Avg. HITRUST e1 score: 99.28	Yes

Section 6 has been truncated for this sample report

HITRUST

Appendix A - Corrective Action Plans Identified

HITRUST requires assessed entities to define corrective action plans (CAPs) for all HITRUST CSF AI Security requirements meeting the following criteria: the requirement's overall score is less than 100 (fully compliant) and the AI Security requirement statements within the associated control reference (e.g., 00.a) averages less than 80. This section lists the CAPs needed to obtain or maintain HITRUST AI Security, 1-year (ai1) Certification.

Requirement	Control Reference	Maturity Score	Corrective Actions (Unvalidated)
BUID: 17.03bAISecOrganizational.3 / CVID: 3052.0 . The organization evaluates the need to take additional measures against AI training data (e.g., adversarial training, using randomized smoothing techniques) to specifically ensure that the machine learning-based AI models it produces are more resistant to evasion and poisoning attacks. This evaluation is documented, performed regularly (at least semiannually) thereafter, and revisited when security incidents related to the AI system occur. Additional measures deemed necessary as a result of this evaluation are implemented by the organization.	03.b Performing Risk Assessments	25.00	*[Status: Not Started, Target Date: 9/15/2025]* We will expand our annual IT security risk assessment approach to incorporate this evaluation.

HITRUST

Appendix B - Additional Gaps Identified

Instances in which a HITRUST CSF requirement scores less than "fully compliant" and the AI security requirement statements 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.

Requirement	Control Reference	Maturity Score
BUID: 15.11cAISecOrganizational.1 | CVID: 3069.0 . The organization's established security incident detection and response processes address the detection of and recovery from AI-specific threats (e.g., poisoning, evasion) through 1. updates to the organization's security incident plans / playbooks; 2. consideration of AI-specific threats in security incident tabletop exercises; 3. recording the specifics of AI-specific security incidents that have occurred; and incorporating 4. logs and 5. alerts from deployed AI systems into the organization's monitoring and security incident detection tools.	11.c Responsibilities and Procedures	75.00

HITRUST

Appendix C – Assessment Results

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

01 Information Protection Program

Related CSF Control	00.a Information Security Management Program
HITRUST CSF Requirement Statement	**BUID: 01.00aAISecOrganizational.1 / CVID: 3038.0 .** As appropriate to the organization's AI deployment context, the stated scope and contents of the organization's written policies, in areas including but not limited to security administration, data governance, software development, risk management, incident management, business continuity, and disaster recovery, explicitly includes the organization's AI systems and their AI specificities.
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.*