HITRUST®

HITRUST CSF® Readiness Assessment Report

Chinstrap Penguin Corp

August 20, 2021

Contents

Section 6 has been truncated for this sample report.

1. 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 global (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 CSF 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 CSF 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.

2. Letter of Readiness Assessment

August 20, 2021

Chinstrap Penguin Corp
1234 Beach View Avenue
Las Vegas, NV 89103

Based upon representation from management as to the accuracy and completeness of information provided in HITRUST's MyCSF® assessment platform, the following platform, facilities, and supporting infrastructure of the organization are v9.4 HITRUST CSF readiness assessed:

Platforms:

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

Facilities:

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

HITRUST® defines two levels of assurance for assessments performed under the HITRUST CSF Assurance Program: Readiness Assessment and Validated Assessment. The type of assessment performed for the above scope is a readiness assessment.

The readiness assessment utilizes a questionnaire aligned with the compliance requirements of the industry. The scores contained in this report are self-reported. The following page of this report contains a representation letter from management where they are asserting to the controls that are in place. However, no testing was performed by an Authorized External Assessor Organization or by HITRUST to validate the results provided by the organization. A completed questionnaire in MyCSF was sent to HITRUST for review and inclusion in the assessment report.

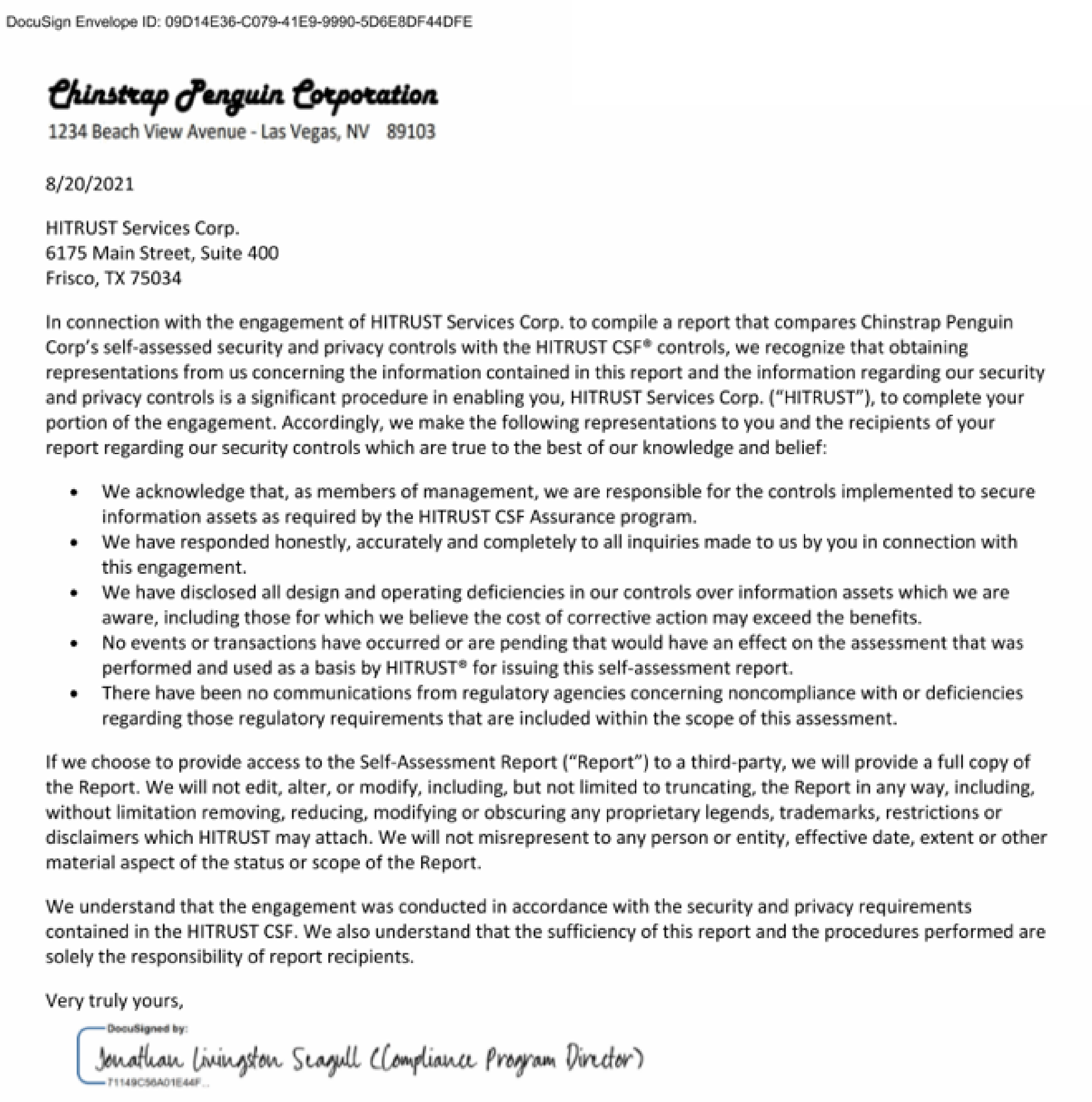
HITRUST CSF readiness assessments allow assessed entities and their stakeholders to realize the benefits of aligning with the HITRUST CSF and leveraging HITRUST's common reporting processes and tools. HITRUST CSF readiness assessments are designed to occur along an incremental path towards certification. Organizations can actively move along the path towards becoming HITRUST CSF Certified in a measured way, while realizing at an early stage the benefits of a common means to assess security controls and communicate compliance.

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

HITRUST

HITRUST

3. Representation Letter from Management



DocuSign Envelope ID: 09D14E36-C079-41E9-9990-5D6E8DF44DFE

Chinstrap Penguin Corporation
1234 Beach View Avenue - Las Vegas, NV 89103

8/20/2021

HITRUST Services Corp.
6175 Main Street, Suite 400
Frisco, TX 75034

In connection with the engagement of HITRUST Services Corp. to compile a report that compares Chinstrap Penguin Corp's self-assessed security and privacy controls with the HITRUST CSF® controls, we recognize that obtaining representations from us concerning the information contained in this report and the information regarding our security and privacy controls is a significant procedure in enabling you, HITRUST Services Corp. ("HITRUST"), to complete your portion of the engagement. Accordingly, we make the following representations to you and the recipients of your report regarding our security controls which are true to the best of our knowledge and belief:

- We acknowledge that, as members of management, we are responsible for the controls implemented to secure information assets as required by the HITRUST CSF Assurance program.
- We have responded honestly, accurately and completely to all inquiries made to us by you in connection with this engagement.
- We have disclosed all design and operating deficiencies in our controls over information assets which we are aware, including those for which we believe 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 this self-assessment report.
- There have been no communications from regulatory agencies concerning noncompliance with or deficiencies regarding those regulatory requirements that are included within the scope of this assessment.

If we choose to provide access to the Self-Assessment Report ("Report") to a third-party, we will provide a full copy of the Report. We will not edit, alter, or modify, including, but not limited to truncating, the Report in any way, including, without limitation removing, reducing, modifying or obscuring any proprietary legends, trademarks, restrictions or disclaimers which HITRUST may attach. We will not misrepresent to any person or entity, effective date, extent or other material aspect of the status or scope of the Report.

We understand that the engagement was conducted in accordance with the security and privacy requirements contained in the HITRUST CSF. We also understand that the sufficiency of this report and the procedures performed are solely the responsibility of report recipients.

Very truly yours,

DocuSigned by:
Jonathan Livingston Seagull (Compliance Program Director)
71149C56A01E44F...

4. Assessment Context

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 CSF Security Assessment

General Factors	
Organization Type	Service Provider (Non-IT)
Entity Type	Non-Healthcare

Geographic Factors	
Geographic scope of operations considered	Multi-State

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?	Yes
Is the system(s) publicly positioned?	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.
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 dial up options in the environment or on any Chinstrap devices.
Is scoped information sent and/or received via fax machine (i.e., an actual machine, excluding efax or scan to email)?	No - There are no fax machines in the environment or fax capabilities on any Chinstrap devices.
Do any of the organization's personnel travel to locations the organization deems to be of significant risk?	No - All Chinstrap employees work in the identified facilities and none of them travel to areas considered to be of significant risk.

Are hardware tokens used as an authentication method within the scoped environment?	No - There are no hardware tokens used within Chinstrap's in-scope environment.
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 - None of the in-scope systems leverage or require the use of e-signatures.
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
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?	Yes
Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component?	Yes
Does the organization use any part of the scoped systems, system components, or system services to sell goods and/or services?	Yes
Is scoped information sent by the organization using courier services, internal mail services, or external mail services (e.g., USPS)?	Yes

Regulatory Risk Factors
Subject to State of Massachusetts Data Protection Act
Subject to the State of Nevada Security of Personal Information Requirements

5. PRISMA Control Maturity Model Overview

HITRUST leverages the concepts and rating scheme of the NISTIR 7358 standard - Program Review for Information Security Management Assistance (PRISMA) to assess an organization's security management program. The methodology is a proven and successful scalable process and approach to evaluating an organization's information security program. The structure of a PRISMA review is based upon the Software Engineering Institute's (SEI) former Capability Maturity Model (CMM), where an organization's developmental advancement is measured by one of five maturity levels. The rating is an indicator of an organization's ability to protect information in a sustainable manner.

Maturity Level	Rating Description
Level 1-	Few if any of the control specifications included in the assessment scope are defined in a policy or standard and may not be implemented as required by the HITRUST CSF.
Level 1	Many of the control specifications included in the assessment scope are defined in a policy or standard but may not be implemented as required by the CSF.
Level 1+	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard but may not be implemented as required by the CSF.
Level 2-	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard but few if any of the requirements are supported with organizational procedures or implemented as required by the CSF.
Level 2	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard, many of the requirements are supported with organizational procedures, but few if any are implemented as required by the CSF.
Level 2+	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard and supported with organizational procedures, but few if any are implemented as required by the CSF.
Level 3-	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard and supported with organizational procedures, and some are implemented as required by the CSF.
Level 3	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard and supported with organizational procedures, and many are implemented as required by the CSF.
Level 3+	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard, supported with organizational procedures, and implemented as required by the CSF.
Level 4-	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard, supported by organizational processes and implemented, and some of these control specifications are routinely measured to ensure they function as intended and as required by the HITRUST CSF.

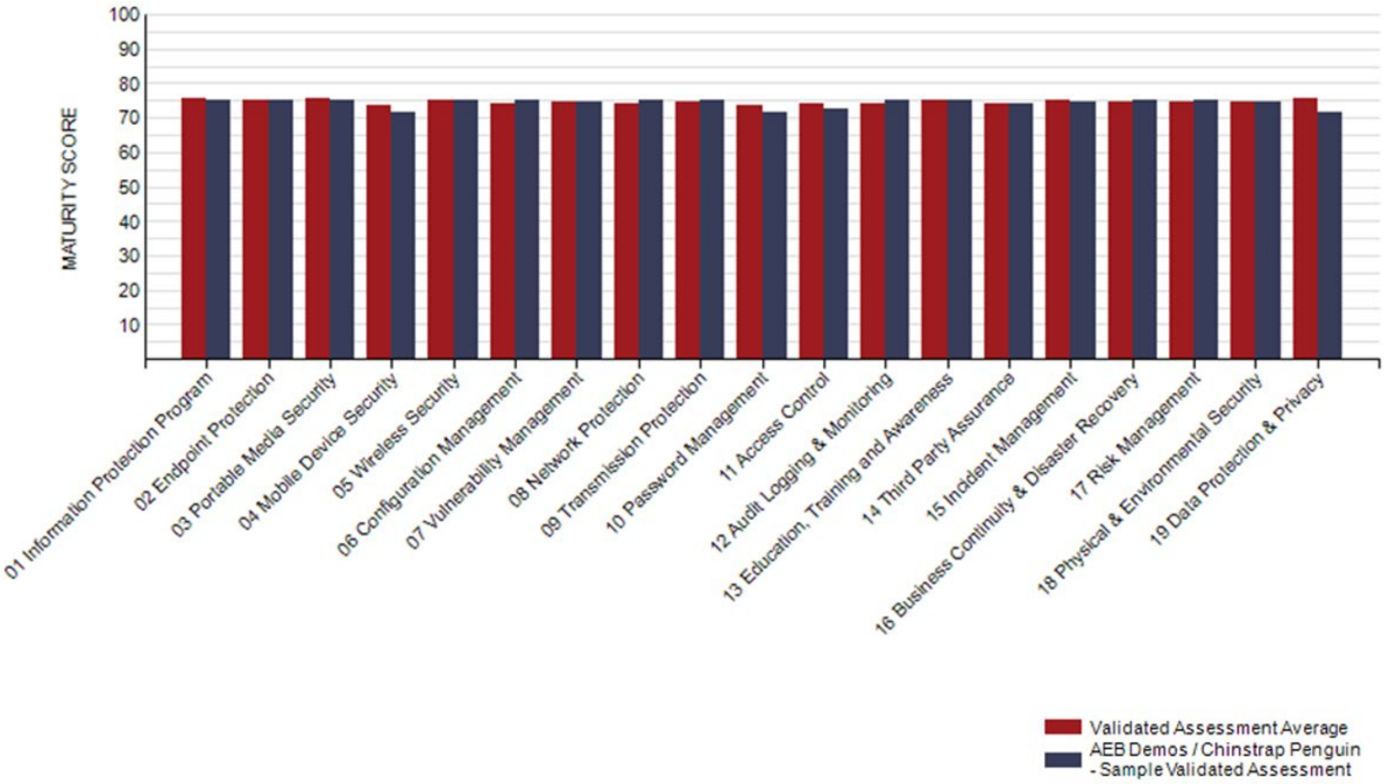
Maturity Level	Rating Description
Level 4	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard, supported by organizational processes and implemented, and many of these control specifications are routinely measured to ensure they function as intended and as required by the HITRUST CSF.
Level 4+	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard, supported by organizational processes, implemented, and routinely measured to ensure they function as intended and as required by the HITRUST CSF.
Level 5-	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard, supported by organizational processes, implemented, and routinely measured, and some are actively managed to ensure they continue to function as intended and as required by the HITRUST CSF.
Level 5	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard, supported by organizational processes, implemented, and routinely measured, and many are actively managed to ensure they continue to function as intended and as required by the HITRUST CSF.
Level 5+	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard, supported by organizational processes, implemented, and routinely measured, and actively managed to ensure they continue to function as intended and as required by the HITRUST CSF.

The HITRUST CSF 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. Each organization's risk management program should define the potential exposure for its business partners and the corresponding assurance required of those controls. The program should also leverage the results of this assessment to evaluate the risks associated with a business relationship and the corresponding risk mitigation strategy. The assessment is not a substitute for a comprehensive risk management program but is a critical data point in the analysis of risk. The assessment should also not be a substitute for management oversight and decision making, but again, leveraged as key input.

The results summarized in this document are based upon a collection of methodologies and tests interacting at a single point in time with technology that is continually changing and becoming ever more complex. Any projection to the future of the findings contained in this document is subject to the risk that, because of change, they may no longer portray the system or environment in existence at that time. The information gathered is subject to inherent limitations and, accordingly, control failures may occur and not be detected.

6. Controls by Assessment Domain

The required controls for certification identified in the HITRUST CSF reflect the controls needed to mitigate the most common sources of breaches. An organization must achieve a rating of "3+" (i.e., a score between 71 and 78) for each assessment domain (control area) to qualify for certification. In some circumstances, a domain reaching a rating of "3" (i.e., a score between 62 and 70) is acceptable if the organization has existing corrective action plans underway.



CSF Assessment Domain	Rating	Comments
01 Information Protection Program	3+	The organization has a formal information protection program based on an accepted industry framework that is reviewed and updated as needed. The information protection program is formally documented and actively monitored, reviewed and updated to ensure program objectives continue to be met.

Section 6 has been truncated for this sample report.

Appendix A - Corrective Action Plans Required for Certification

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 a 71 (3+), the requirement's implemented maturity level scores less than "fully compliant", the associated control reference (e.g., 00.a) is required for certification, and the associated control reference scores less than a 71 (3+). This section lists the CAPs needed to obtain or maintain certification. Remediation of the additional gaps identified (listed in the following section) is not required but is recommended to ensure complete implementation of the HITRUST CSF.

Identifier	Requirement	Control Reference	Maturity Rating	Maturity Level(s) Deficient
1687.1650707	Personnel who telework are trained on the risks, the controls implemented, and their responsibilities.	01.y Teleworking	2+	Process Implementation
1687.1650878	Audit logs of the scans are maintained.	09.j Controls Against Malicious Code	1	Policy Process Implementation
1687.1650675	The organization, based on the data classification level, registers media (including laptops) prior to use, places reasonable restrictions on how such media are used, and provides an appropriate level of physical and logical protection (including encryption) for media containing covered information until properly destroyed or sanitized.	09.o Management of Removable Media	2-	Policy Process Implementation

Appendix B - Additional Gaps Identified

Identifier	Requirement	Control Reference	Maturity Rating	Maturity Level(s) Deficient
1687.1650609	The organization has a formal information protection program based on an accepted industry framework that is reviewed and updated as needed.	00.a Information Security Management Program	2+	Policy Process
1687.1650794	Privileges are formally authorized and controlled, allocated to users on a need-to-use and event-by-event basis for their functional role (e.g., user or administrator), and documented for each system product/element.	01.c Privilege Management	2+	Policy Process Implementation
1687.1650612	Teleworking activities are only authorized if security arrangements and controls that comply with relevant security policies and organizational requirements are in place.	01.y Teleworking	2+	Policy Process
1687.1650743	Prior to authorizing teleworking, the physical security of the teleworking site is evaluated and any threats/issues identified are addressed.	01.y Teleworking	2+	Policy Process
1687.1650885	Suitable protections of the teleworking site are in place to protect against the theft of equipment and information, the unauthorized disclosure of information, and unauthorized remote access to the organization's internal systems or misuse of facilities.	01.y Teleworking	2+	Policy Process
1687.1650672	Anti-virus and anti-spyware are installed, operating and updated on all end-user devices to conduct periodic scans of the systems to identify and remove unauthorized software. Server environments for which the server software developer specifically recommends not installing host-based anti-virus and anti-spyware software are addressed via a network-based malware detection (NBMD) solution.	09.j Controls Against Malicious Code	3-	Policy Process

Identifier	Requirement	Control Reference	Maturity Rating	Maturity Level(s) Deficient
1687.1650889	Quarterly scans are performed to identify unauthorized wireless access points, and appropriate action is taken if any unauthorized access points are discovered.	09.m Network Controls	3-	Policy
1687.1650907	Applications that store, process, or transmit covered information undergo automated application vulnerability testing by a qualified party on an annual basis.	10.b Input Data Validation	2+	Policy Process