HITRUST Risk-based, 2-year (r2) Certification Report

Chinstrap Penguin Corp.

August 20, 2021

HITRUST®

HITRUST

Contents

Section 9 and Appendix C have been truncated for this sample report.

HITRUST

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 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*

HITRUST

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

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, the procedures performed by an Authorized External Assessor to validate such information, and HITRUST's independent confirmation that the work was performed in accordance with the HITRUST® Assurance Program requirements, the following platform, facilities, and supporting infrastructure of the Organization ("Scope") meet the HITRUST CSF® v9.1 Risk-based, 2-year (r2) certification criteria:

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

The certification is valid for a period of two years assuming the following occurs:

- Annual progress is being made on areas identified in the Corrective Action Plan(s) (CAPs),
- No data security breach reportable to a federal or state agency by law or regulation has occurred,
- No significant changes in the business or security policies, practices, controls, and processes have occurred that might impact its ability to meet the HITRUST Risk-based, 2-year (r2) certification criteria, and
- Timely completion of the HITRUST Interim Assessment for r2 Certification as defined in the HITRUST Assurance Program Requirements.

HITRUST has developed the HITRUST CSF, a certifiable framework that provides organizations with the needed structure, detail and clarity relating to information protection. With input from leading organizations, HITRUST identified a subset of the HITRUST CSF control requirements that an organization must meet to be HITRUST Risk-based, 2-year (r2) Certified. For certain

HITRUST CSF control requirements that were not being met, the Organization developed a CAP that outlined its plans for meeting such requirements.

HITRUST performed a quality assurance review to ensure that the control maturity scores were consistent with the results of testing performed by the Authorized External Assessor. In addition to the full report that follows, users of the report can refer to the document *Leveraging HITRUST CSF Assessment Reports: A Guide for New Users* for questions on interpreting the results contained herein and can contact HITRUST customer support at *support@hitrustalliance.net.* Users of this report are assumed to be familiar with and understand the services provided by the organization listed above, and what specific services are being used by the user organization.

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

HITRUST

HITRUST

3. Representation Letter from Management

DocuSign Envelope ID: 7E50EA76-1CA6-4F61-B8D4-0C483BF5D02C

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 our engagement to perform an assessment of Chinstrap Penguin Corp's information protection controls compared with the HITRUST CSF® controls included in the scope of the assessment, we recognize that obtaining representations from us concerning the information contained in this report and the information regarding our information protection controls is a significant procedure in enabling you, HITRUST Services Corporation ("HITRUST"), to complete your portion of the engagement. Accordingly, we make the following representations to you and the recipients of your report regarding our information protection controls which are true to the best of our knowledge and belief:

- We acknowledge that, as members of management, we are responsible for the implementation of information protection controls as required by HITRUST.
- We have responded honestly, accurately and completely to all inquiries made to us during the engagement.
- We have made available to the HITRUST External Assessor all records and necessary documentation related to the information protection controls included within the scope of this engagement.
- We have disclosed all design and operating deficiencies in our information protection controls 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 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 engagement.

We understand that the engagement was conducted in accordance with the requirements outlined by HITRUST in performing assessments utilizing the HITRUST CSF. We also understand that evaluating the sufficiency of this report and the procedures performed are solely the responsibility of report recipients.

Regards,

DocuSigned by:
Jonathan Livingston Seagull (Compliance Program Director)
7114BC56A01E44F...

HITRUST

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, systematic, and regulatory risk factors.

Assessment Type
HITRUST CSF Security Assessment (r2 Validated)

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

Systematic 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/business partner?	Yes
Is the system(s) accessible from a public location?	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 - 85,000
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 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 personally owned devices to connect to scoped organizational assets (i.e., BYOD - bring your own device)?	Yes
Does the organization use any part of the scoped systems, system components, or system services to sell goods and/or services?	Yes
Does the organization allow the use of electronic signatures to provide legally binding consent within the scoped environment, e.g., simple or basic electronic signatures (SES), advanced electronic or digital signature (AES), or qualified advanced electronic or digital signatures (QES)?	No - None of the in-scope systems leverage or require the use of e-signatures.
Is scoped information sent by the organization using courier services, internal mail services, or external mail services (e.g., USPS)?	Yes
Does the system allow users to access the scoped environment from an external network that is not controlled by the organization?	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

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

HITRUST

5. 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 Platforms

The following table presents the platforms that were 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(s) Type(s)	Oracle
Operating System(s)	HP-UX
Residing Facility	Pelican Data Center
Exclusions 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 tables present the facilities that were included in the scope of this assessment.

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

Services Outsourced

The following table presents outsourced services relevant to the scope of this assessment.

The "Consideration in this Assessment" column of the following table specifies the method utilized for each service provider relevant to the scope of this r2 assessment. HITRUST requires that the inclusive method be used on all r2 assessments but allows use of both the inclusive and exclusive methods on HITRUST Implemented, 1-year (i1) validated assessments.

Organizations undergoing i1 validated assessments have two options of how to address situations in which a HITRUST CSF requirement is fully or partially performed by a service provider (e.g. by a cloud service provider):

- The Inclusive method, whereby HITRUST CSF requirements performed by the service provider are included within the scope of the i1 assessment and addressed through full or partial inheritance, reliance on third-party assurance reports, and/or direct testing, and

- The Exclusive (or Carve-out), method, whereby HITRUST CSF requirements performed by the service provider are excluded from the scope of the i1 assessment and marked as N/A with supporting commentary that specifies that the HITRUST CSF requirement is fully performed by a party other than the assessed entity (for fully outsourced controls) or through commentary describing the excluded partial performance of the control (for partially outsourced controls).

Third-party Provider	Relevant Service(s) Provided	Consideration in this Assessment
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

Overview of the Security Organization

Chinstrap's information security function is housed under the larger information technology department. The information security function is led by the CISO who reports to the CIO. The information security function has developed a robust information security program focused on managing information security risk. Key elements of the program include:

- Risk management
- Network security
- Application security
- Physical security
- Business continuity and disaster recovery

- Incident management
- Identity and access management
- Compliance management
- Security training and awareness

HITRUST

6. Procedures Performed by the External Assessor

An Authorized HITRUST CSF External Assessor Organization (i.e., the external assessor) performed procedures to validate the assessed entity's asserted control maturity scores. These validation procedures were designed by the external assessor based upon the assessment's scope in observance of HITRUST's Assurance Program Requirements and consisted of inquiry with key personnel, inspection of system-generated evidence (e.g., access lists, logs, configurations, sample items), on-site or virtual observations, and (optionally) reperformance of controls.

For certain portions of the assessment and as allowed by HITRUST's Assurance Program requirements, the external assessor may have utilized the work of other assessors, auditors, and/or inspectors in lieu of direct testing. All assessment procedures performed by the external assessor, including those where the external assessor utilized the work of others, were subject to HITRUST's quality assurance review procedures. The table below details assessments utilized by the external assessor.

Potential options available for using the work of others allowed by HITRUST's Assurance Program Requirements include the following and are reflected in the "Utilization Approach" column of the below table:

- Inheritance of results or reliance upon another validated HITRUST CSF assessment,
- Reliance on audits and/or assessments performed by a third party, and/or
- Reliance on testing performed by the assessed entity (i.e. by internal assessors).

Assessment Utilized	Assessed Entity	Assessment Type	Report Date(s)	Utilization Approach	Relevant Platforms	Relevant Facilities	Assessment Domains
Pelican Hosting SOC 2 Type II	Pelican Hosting	Period-of-time assessment report (e.g. SOC 2 Type II)	*Issuance Date:* 05/27/2021 *Report Period:* 10/1/2020 – 4/30/2021	Reliance	Customer Central (a.k.a. "Portal")	Pelican Data Center	18 Physical & Environmental Security

HITRUST

7. 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	Scoring Range	Rating Description
Level 1-	0 – 9	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	10 – 18	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+	19 – 26	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-	27 – 35	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	36 – 44	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+	45 – 52	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-	53 – 61	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	62 – 70	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+	71 – 78	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.

Maturity Level	Scoring Range	Rating Description
Level 4-	79 – 82	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.
Level 4	83 – 86	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+	87 – 89	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-	90 – 93	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	94 – 97	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+	98 – 100	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 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.

HITRUST

8. Results by Control Reference

To assist organizations with prioritizing and focusing efforts, HITRUST established a list of priority controls based on an analysis of breach data and input obtained from over 100 security professionals. By implementing these controls, organizations mitigate threats and exposures that are most likely to result in a breach. An organization must implement these controls to qualify for HITRUST Risk-based, 2-year (r2) Certification.

The following table is a summary of the results for Chinstrap Penguin Corp of the testing of required controls:

Control Reference	Maturity Score of 71 or Higher	Requirement with Corrective Action Plan (CAP)	CAP Identifier
00.a Information Security Management Program	Yes	None	N/A
01.b User Registration	Yes	None	N/A
01.c Privilege Management	Yes	None	N/A
01.d User Password Management	Yes	None	N/A
01.e Review of User Access Rights	Yes	None	N/A
01.h Clear Desk and Clear Screen Policy	Yes	None	N/A
01.j User Authentication for External Connections	Yes	None	N/A
01.l Remote Diagnostic and Configuration Port Protection	Yes	None	N/A
01.m Segregation in Networks	Yes	None	N/A
01.n Network Connection Control	Yes	None	N/A
01.o Network Routing Control	Yes	None	N/A
01.q User Identification and Authentication	Yes	None	N/A
01.t Session Time-out	Yes	None	N/A

Control Reference	Maturity Score of 71 or Higher	Requirement with Corrective Action Plan (CAP)	CAP Identifier
01.v Information Access Restriction	Yes	None	N/A
01.w Sensitive System Isolation	Yes	None	N/A
01.x Mobile Computing and Communications	Yes	None	N/A
01.y Teleworking	No	Personnel who telework are trained on the risks, the controls implemented, and their responsibilities.	1687.1650707
02.a Roles and Responsibilities	Yes	None	N/A
02.d Management Responsibilities	Yes	None	N/A
02.e Information Security Awareness, Education, and Training	Yes	None	N/A
02.f Disciplinary Process	Yes	None	N/A
02.i Removal of Access Rights	Yes	None	N/A
03.b Performing Risk Assessments	Yes	None	N/A
03.c Risk Mitigation	Yes	None	N/A
03.d Risk Evaluation	Yes	None	N/A
04.a Information Security Policy Document	Yes	None	N/A
04.b Review of the Information Security Policy	Yes	None	N/A
05.a Management Commitment to Information Security	Yes	None	N/A
05.h Independent Review of Information Security	Yes	None	N/A
05.i Identification of Risks Related to External Parties	N/A	None	N/A
05.j Addressing Security When Dealing with Customers	Yes	None	N/A

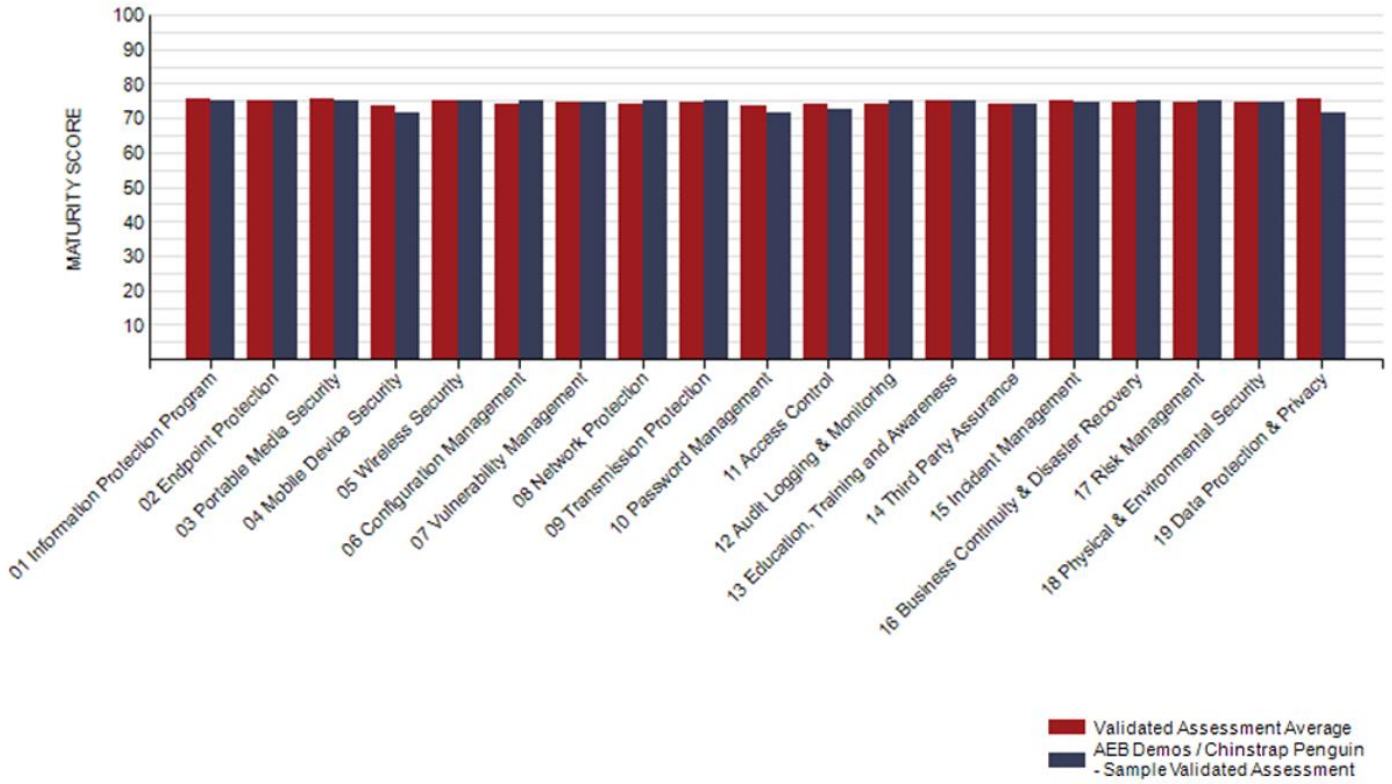
Control Reference	Maturity Score of 71 or Higher	Requirement with Corrective Action Plan (CAP)	CAP Identifier
05.k Addressing Security in Third Party Agreements	Yes	None	N/A
06.c Protection of Organizational Records	Yes	None	N/A
06.d Data Protection and Privacy of Covered Information	Yes	None	N/A
06.e Prevention of Misuse of Information Assets	Yes	None	N/A
06.g Compliance with Security Policies and Standards	Yes	None	N/A
06.h Technical Compliance Checking	Yes	None	N/A
07.a Inventory of Assets	Yes	None	N/A
07.c Acceptable Use of Assets	Yes	None	N/A
08.b Physical Entry Controls	Yes	None	N/A
08.d Protecting Against External and Environmental Threats	Yes	None	N/A
08.j Equipment Maintenance	Yes	None	N/A
08.l Secure Disposal or Re-Use of Equipment	Yes	None	N/A
09.aa Audit Logging	Yes	None	N/A
09.ab Monitoring System Use	Yes	None	N/A
09.ad Administrator and Operator Logs	Yes	None	N/A
09.b Change Management	Yes	None	N/A
09.c Segregation of Duties	Yes	None	N/A
09.e Service Delivery	Yes	None	N/A
09.f Monitoring and Review of Third-party Services	Yes	None	N/A

Control Reference	Maturity Score of 71 or Higher	Requirement with Corrective Action Plan (CAP)	CAP Identifier
09.j Controls Against Malicious Code	No	Audit logs of the scans are maintained.	1687.1650878
09.k Controls Against Mobile Code	Yes	None	N/A
09.l Back-up	Yes	None	N/A
09.m Network Controls	Yes	None	N/A
09.n Security of Network Services	Yes	None	N/A
09.o Management of Removable Media	No	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.	1687.1650675
09.p Disposal of Media	Yes	None	N/A
09.q Information Handling Procedures	Yes	None	N/A
09.s Information Exchange Policies and Procedures	Yes	None	N/A
09.v Electronic Messaging	Yes	None	N/A
09.x Electronic Commerce Services	Yes	None	N/A
09.y On-line Transactions	Yes	None	N/A
10.a Security Requirements Analysis and Specification	Yes	None	N/A
10.b Input Data Validation	Yes	None	N/A
10.f Policy on the Use of Cryptographic Controls	Yes	None	N/A
10.h Control of Operational Software	Yes	None	N/A
10.k Change Control Procedures	Yes	None	N/A
10.l Outsourced Software Development	Yes	None	N/A

Control Reference	Maturity Score of 71 or Higher	Requirement with Corrective Action Plan (CAP)	CAP Identifier
10.m Control of Technical Vulnerabilities	Yes	None	N/A
11.a Reporting Information Security Events	Yes	None	N/A
11.c Responsibilities and Procedures	Yes	None	N/A
11.d Learning from Information Security Incidents	Yes	None	N/A
12.b Business Continuity and Risk Assessment	Yes	None	N/A
12.c Developing and Implementing Continuity Plans Including Information Security	Yes	None	N/A
12.d Business Continuity Planning Framework	Yes	None	N/A

9. Results by Assessment Domain

The required controls for HITRUST Risk-based, 2-year (r2) certification identified in the HITRUST CSF reflect the controls needed to mitigate the most common sources of breaches. An organization must achieve a straight average score of at least 71 for each assessment domain to qualify for HITRUST Risk-based, 2-year (r2) certification. Assessment domains with straight averages as low as 62 are acceptable if the organization has existing corrective action plans underway. 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.



CSF Assessment Domain	Maturity Score	Fully Implemented HITRUST CSF Requirements
01 Information Protection Program	76	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 9 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 requirements meeting the following criteria: the requirement's overall score is less than 71, the requirement's implemented maturity level scores less than "fully compliant", the associated control reference (e.g., 00.a) is required for HITRUST Risk-based, 2-year (r2) certification, and the associated control reference averages less than 71. This section lists the CAPs needed to obtain or maintain HITRUST Risk-based, 2-year (r2) certification.

Identifier	Requirement	Control Reference	Maturity Score	Maturity Level(s) Deficient	Point of Contact (POC)	Scheduled Completion Date	Corrective Actions	Status
1687.1650707	Personnel who telework are trained on the risks, the controls implemented, and their responsibilities.	01.y Teleworking	55	Process Implementation	Training Department	10/27/2021	Implemented: The teleworking training material will be updated to address the risks, controls implemented, and user responsibilities related to teleworking.	Not Started
1687.1650878	Audit logs of the scans are maintained.	09.j Controls Against Malicious Code	44	Policy Process Implementation	IT	3/25/2022	Policy & Procedures: The Anti-Malware Policy and Procedure document will be updated to include policy and procedure around the checking of anti-virus or anti-spy software (e.g., anti-malware) generates audit logs of checks performed. Implemented: The organization will ensure that evidence	Started - On Track

Identifier	Requirement	Control Reference	Maturity Score	Maturity Level(s) Deficient	Point of Contact (POC)	Scheduled Completion Date	Corrective Actions	Status
							of anti-malware audit logs are available for the external assessor to test.	
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	33	Policy Process Implementation	IT	12/2/2021	Policy and Procedure: The Portable Media Security Policy and Procedure document will be updated to include (i) restrictions on the type(s) of media, and usages thereof to maintain security; and, (ii) registration of certain type(s) of media including laptops. Implemented: The organization will implement monthly reviews to ensure that all new portable media is appropriately registered and documented.	Not Started

HITRUST

Appendix B - Additional Gaps Identified

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

Identifier	Requirement	Control Reference	Maturity Score	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	56	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	44	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	58	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	19	Policy Process

HITRUST

Appendix C - Assessment Results

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

01 Information Protection Program

Related CSF Control	00.a Information Security Management Program		
HITRUST CSF Requirement Statement	The organization has a formal information protection program based on an accepted industry framework that is reviewed and updated as needed.		
Your Maturity Assessment	Policy 5. Fully Compliant (100%)	Process 5. Fully Compliant (100%)	Implemented 5. Fully Compliant (100%)
Maturity Score	75		

Related CSF Control	00.a Information Security Management Program		
HITRUST CSF Requirement Statement	The information protection program is formally documented and actively monitored, reviewed and updated to ensure program objectives continue to be met.		
Your Maturity Assessment	Policy 5. Fully Compliant (100%)	Process 5. Fully Compliant (100%)	Implemented 5. Fully Compliant (100%)
Maturity Score	75		

Appendix C has been truncated for this sample report.