HITRUST Implemented, 1-year (i1) Certification Report

Chinstrap Penguin Corp.

January 20, 2022

HITRUST®

HITRUST

Contents

Some sections 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 Implemented, 1-year (i1) Certification

January 20, 2022

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® v9.6 Implemented, 1-year (i1) 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 one year assuming the following occurs:

- No data security breach reportable to a federal or state agency by law or regulation has occurred, 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 Implemented, 1-year (i1) certification criteria.

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 Implemented, 1-year (i1) Certified. For certain HITRUST CSF control requirements that were not being met, the Organization developed a corrective action plan (CAP) that outlined its plans for meeting such requirements.

HITRUST performed a quality assurance review to ensure that the implementation 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 contact HITRUST customer support at *support@hitrustalliance.net* for questions on interpreting the results contained herein. 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

3. Representation Letter from Management

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

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

1/20/2022

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...

4. Assessment Context

HITRUST historically offered only one information protection certification, the HITRUST CSF Certification, achievable only by demonstrating sufficiently strong control maturity through the performance of a validated assessment. By design, this HITRUST certification offered a gold-standard level of assurance due to the comprehensive control requirements and assurance program requirements. However, completion of this HITRUST validated assessment was a significant undertaking for many organizations.

HITRUST acknowledged that the highest level of information protection assurance was not needed by every organization or vendor relationship and that a broader range of certification options was necessary to address varying assurance requirements and needs—as determined by factors such as level of effort, budget, and purpose. To address these needs, HITRUST introduced an assessment mechanism and accompanying certification that is less effort and cost than the typical HITRUST validated assessment while still living up to the gold standard level of quality for which HITRUST certifications are known: the *HITRUST Implemented, 1-year (i1) Certification*. To differentiate the two certifications, HITRUST also renamed the existing certification to the *HITRUST Risk-based, 2-year (r2) Certification*.

The *HITRUST Risk-based, 2-year (r2) Certification* continues to provide the highest level of information protection assurance for situations with greater risk exposure due to data volumes, regulatory compliance, or other risk factors. The *HITRUST Implemented, 1-year (i1) Certification* provides, when compared to the r2, a relatively moderate level of information protection assurance, focusing on good security hygiene and cybersecurity best practices controls.

The *HITRUST Implemented, 1-year (i1) Certification* shares several similarities with the *HITRUST Risk-based, 2-year (r2) Certification*. Both provide a means to convey information assurances over the assessed entity's scoped control environment through a shareable, final report with certification issued by HITRUST. And, both require an Authorized HITRUST External Assessor Organization to inspect documented evidence to validate control implementation.

The i1 and r2 are distinct in many ways, however. r2 certifications can be valid for 2 years, while i1 certifications can be valid for 1 year. Also, many control maturity levels (policy, process, implemented, and optionally measured and managed) are considered when scoring HITRUST CSF requirements included in r2 assessments, while the scoring of HITRUST CSF requirements included in i1 assessments considers only control implementation. Further, while the HITRUST CSF requirements considered in r2 assessments are customized based on the assessed entity's risk inherent factors (e.g., whether in-scope systems are accessible from the Internet, whether wireless networks are used in the scoped environment) or optional inclusion of authoritative sources (e.g., HIPAA Privacy Rule, PCI DSS), the HITRUST CSF requirements in an i1 assessment are carefully curated by HITRUST.

HITRUST Implemented, 1-year assessments consider good security hygiene controls and cybersecurity best-practice controls, and this design affords a high degree of coverage against authoritative sources generally viewed as security best practices. As a result, the HITRUST

CSF requirements included in i1 assessments provide a high degree of coverage against sources such as the HIPAA Security Rule; NIST SP 800-171; the NAIC Data Security Law; the FTC's GLBA Safeguards Rule (both the current version as well as the 2021 proposed update); NISTIR 7621: Small Business Information Security Fundamentals; the DOL's EBSA Cybersecurity Program Best Practices; and the HITRUST CSF requirements included in HITRUST's Basic, Current-state (bC) assessment.

The i1 was also designed to be an evolving, threat-adaptive assessment and accompanying certification that leverages threat intelligence and best practice controls to deliver an assessment that addresses relevant practices and active cyber threats. HITRUST continually evaluates cybersecurity controls to identify those relevant to mitigating known risks through the use of cyber threat intelligence data from leading threat intelligence providers. As a result, the i1 includes controls that were selected exclusively to address emerging cyber threats actively being targeted today.

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, now offering 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 tables present 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 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 i1 assessment. Organizations undergoing HITRUST Implemented, 1-year (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).

HITRUST requires that the inclusive method be used on all HITRUST Risk-based, 2-year validated assessments but allows use of both the inclusive and exclusive methods on i1 assessments such as the one underlying this report.

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
Seashore Offsite Data Storage	Seashore provides backup tape delivery and storage in a secure offsite facility. No customer, covered, or otherwise confidential information is stored at Seashore's facilities, however.	Excluded

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. Use of the Work of Others

For certain portions of the assessment and as allowed by HITRUST's Assurance Program Requirements, the external assessor 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 HITURST'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	*Issuance Date:* 05/27/2021 *Report Period:* 10/1/2020 – 4/30/2021	Reliance on a third-party assurance report	Customer Central (a.k.a. "Portal")	Pelican Data Center	18 Physical & Environmental Security

HITRUST

7. Assessment Approach

An Authorized HITRUST CSF 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 CSF Assurance Program Requirements and consisted of inquiry with key personnel, inspection of evidence (e.g. access lists, logs, configuration, sample items, policies, procedures, diagrams), on-site or virtual observations, (optionally) utilization of the work of others (as described in Section 6 of 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:

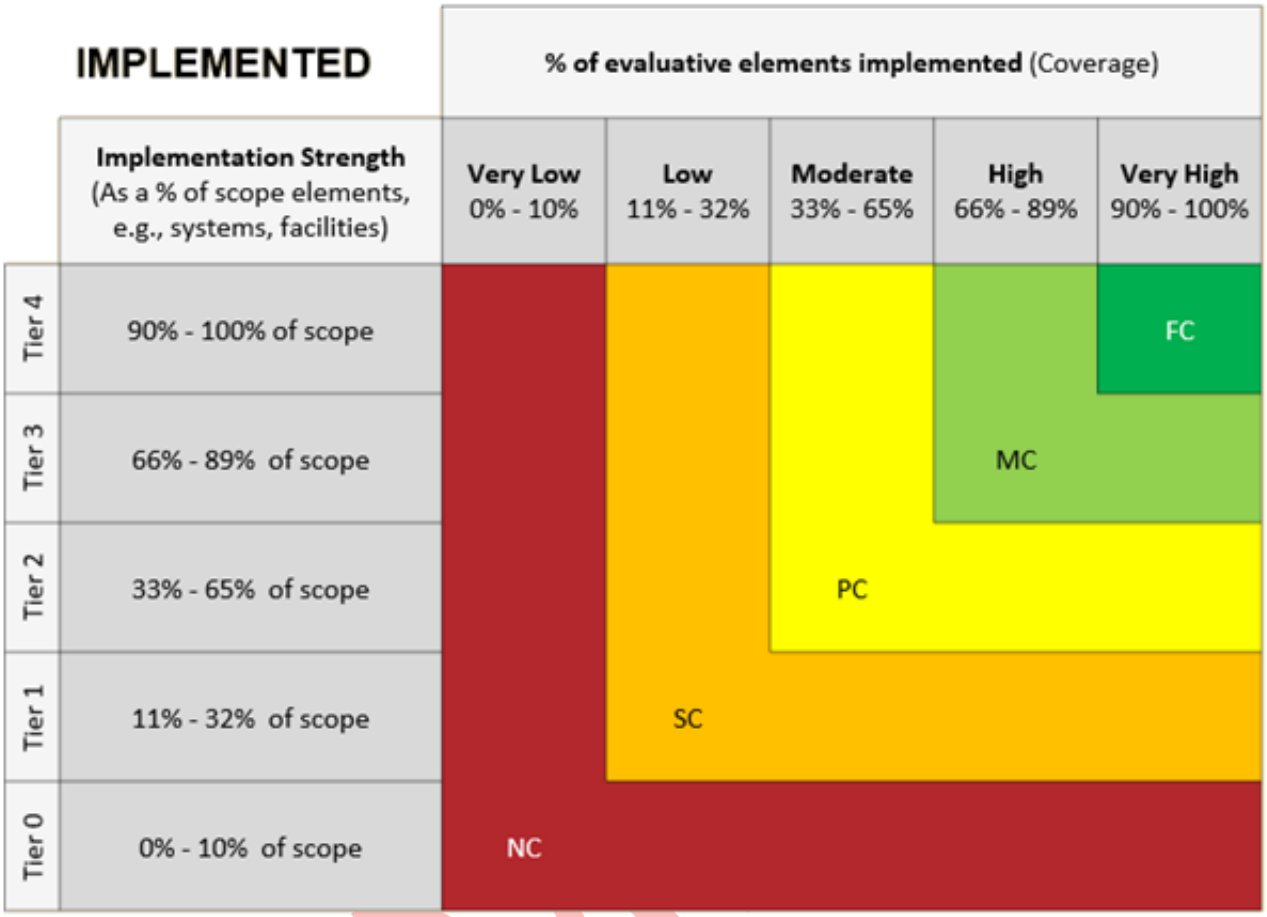
- The HITRUST CSF requirement's implementation **strength** is evaluated using a 5-point scale (tier 0 through tier 4) by considering the requirement's implementation and operation across the assessment scope, which consists of all organizational and system elements, including the physical facilities and logical systems / platforms, within the defined scope of the i1 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 i1 assessments incorporates the following scale. The overall score for each HITRUST CSF requirement ranges from 0 to 100 points in quartile increments based directly on the requirement's implementation score.

Implementation Score	Description	Points Awarded
Non-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

The section of the HITRUST scoring rubric used to determine implementation scoring is as follows:



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. 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

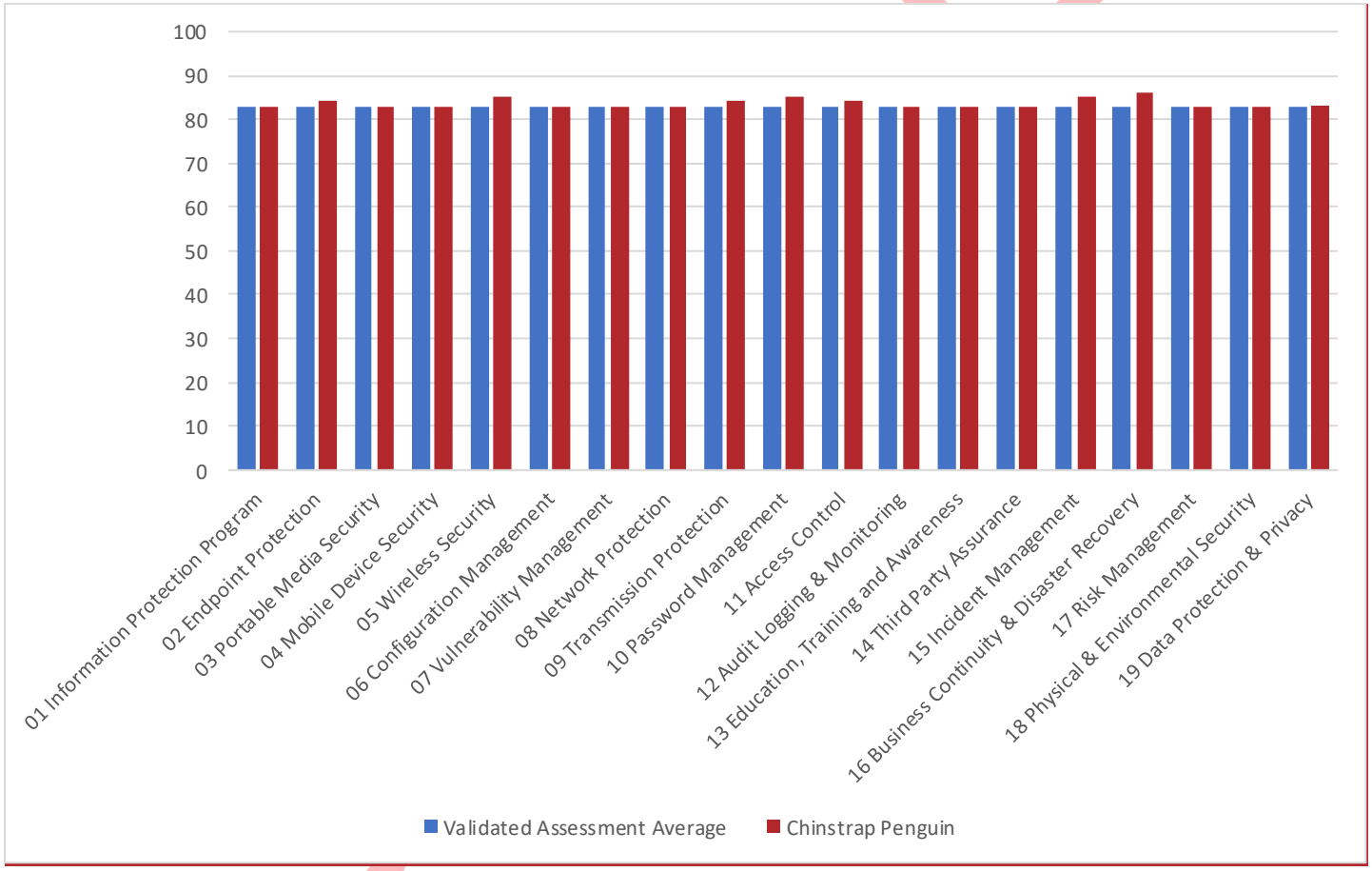
Each HITRUST CSF requirement is associated with a HITRUST CSF control reference. The following table is a control reference-level summary of the results for this assessment. Details of each identified CAP can be found in Appendix A of this report.

Control Reference	Average Score 80 or Higher?	HITRUST CSF Requirement with Corrective Action Plan (CAP)	CAP Identifier
00a- Information Security Management Program	Yes	The organization has a formal information protection program based on an accepted industry framework that is reviewed and updated as needed.	12345.123
01a- Access Control Policy	Yes	None	N/A
01b- User Registration	Yes	None	N/A
01c- Privilege Management	Yes	None	N/A
01d- User Password Management	Yes	None	N/A
01e- Review of User Access Rights	Yes	None	N/A
01h- Clear Desk and Clear Screen Policy	Yes	Covered or critical business information is not left unattended or available for unauthorized individuals to access, including on desks, printers, copiers, fax machines, and computer monitors.	12345.456
01i- Policy on the Use of Network Services	Yes	None	N/A
01j- User Authentication for External Connections	Yes	None	N/A
01l- Remote Diagnostic and Configuration Port Protection	Yes	None	N/A
01m- Segregation in Networks	Yes	None	N/A
01n- Network Connection Control	Yes	None	N/A
01o- Network Routing Control	Yes	None	N/A
01p- Secure Log-on Procedures	Yes	None	N/A

Section 8 has been truncated in this sample report.

9. Results by Assessment Domain

Each HITRUST CSF requirement is associated with one of 19 assessment domains. An organization must achieve a straight-average score of at least 83 for each assessment domain to qualify for HITRUST i1 certification.



Assessment Domain	Average Score	Fully Implemented Requirements
01 Information Protection Program	83	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. The organization has an information security workforce improvement program. Management ensures users are(i) briefed on their security role(s)/responsibilities, conform with the terms and conditions of employment prior to obtaining access to the organization's information systems; (ii) provided with guidelines regarding the security expectations of their roles; (iii) motivated to comply with security policies; and, (iv) continue to have the appropriate skills and qualifications for their role(s). The organization conducts screening before authorizing access to information resources. If the senior-level information security official is employed by the organization, one of its affiliates, or a third-party service, the organization retains responsibility for its cybersecurity program, designates a senior member of the organization responsible for direction and oversight, and requires the third-party service to maintain an appropriate cybersecurity program of its own. The CISO of the organization reports in writing on the organization's cybersecurity program and material cybersecurity risks, at least annually, to the organization's board of directors, equivalent governing body, or suitable committee. Information security objectives, approach, scope, importance, goals, and principles for the organization's security program are formally identified, communicated throughout the organization to users in a form that is relevant, accessible, and understandable to the intended reader; and supported by a controls framework that considers legislative, regulatory, contractual requirements, and other policy-related requirements.

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 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 Implemented, 1-year (i1) certification:

Identifier	Requirement	Associated Control Reference	Score	Point of Contact (POC)	Scheduled Completion Date	Corrective Actions	Status
12345.123	The organization has a formal information protection program based on an accepted industry framework that is reviewed and updated as needed.	00a- Information Security Management Program	52	CISO	10/27/2021	The organization will align its security program efforts with an accepted industry framework.	Not Started
12345.456	Covered or critical business information is not left unattended or available for unauthorized individuals to access, including on desks, printers, copiers, fax machines, and computer monitors.	01h- Clear Desk and Clear Screen Policy	47	Operations Management	3/25/2022	The organization will implement a badge-swipe requirement in order to complete print jobs on shared printers in the corporate HQ.	Started - On Track

HITRUST

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 if a CAP. Remediation of the additional gaps identified is not required but is strongly recommended. The gaps identified in this assessment are as follows:

Identifier	HITRUST CSF Requirement	Associated Control Reference	Requirement Score
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	50
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	50

Appendix B has been truncated for this sample report.

HITRUST

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	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.
Implemented 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.
Implemented Score	75

Appendix C has been truncated for this sample report.