HITRUST Essentials, 1-year (e1) Certification Report

Chinstrap Penguin Corp.

Valid for the period
January 26, 2023 - January 26, 2024

EXAMPLE

HITRUST®

HITRUST

Contents

This table of contents has 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.*

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

January 26, 2023

Chinstrap Penguin Corp.
123 Main St
Las Vegas, NV 78026-4303

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, facility, and supporting infrastructure of the Organization ("Scope") meets the HITRUST CSF® v11.0 Essentials, 1-year (e1) certification criteria:

Platform:

- 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
- Headquarters and Manufacturing located in Las Vegas, Nevada, United States of America
- 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. 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 data security breach reportable to a federal or state agency by law or regulation has occurred within or affecting the assessed environment, 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 Essentials, 1-year (e1) 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 requirements that an organization must meet to be HITRUST Essentials, 1-year (e1) Certified.

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 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: 2008A83B-1EAE-4D11-97A1-E86D07F7F15D

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

1/26/2023

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

In connection with our engagement to perform an assessment of testing'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 information protection controls implemented as required by the HITRUST.
- We have responded honestly, accurately and completely to all inquiries made to us during the engagement.
- We have made available to the HITRUST CSF 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 assessment.

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)
DA8CA97CC10F4D8...

4. Assessment Context

HITRUST Essentials, 1-year assessments address the need for a continuously-relevant cybersecurity assessment focusing on foundational cybersecurity controls and mitigations for the most pressing cybersecurity threats. Organizations successfully achieving a e1 certification can reliably demonstrate they meet a bar of essential cybersecurity hygiene.

This assessment is designed for lower assurance scenarios (such as those needing greater assurances than achieved through information security questionnaires or readiness assessments but less so than those achieved through more robust, higher effort assessments). However, an e1 assessment can also serve as a starting point for enterprises that are in the early stages of implementing their information security controls.

To ensure foundational cybersecurity is in place, e1 assessments focuses on a pre-set selection of HITRUST CSF requirements curated by HITRUST. While not a compliance assessment, the subject matter does overlap with authoritative sources sharing similar goals (such as CISA Cyber Essentials, Health Industry Cybersecurity Practices (HICP) for Small Healthcare Organizations, NIST SP 800-171's "Basic" requirements, and NIST IR 7621: Small Business Information Security Fundamentals.

HITRUST's analysis of cyber threat intelligence data from leading threat intelligence providers when curating the controls considered during e1 assessments, e1 is an evolving, threat-adaptive assessment. HITRUST continually evaluates this data in relation to the controls included in the e1 to ensure that the e1 continues to address the most critical cyber threats (such as ransomware, phishing, brute force, and abuse of valid accounts).

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 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 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.

Customer Central (a.k.a. "Portal")	
Application(s)	The applications/service offerings that make up the Portal are Penguin Nest, Penguin Analytics, and South Pole Benefit Eligibility.
Database Type(s)	Oracle
Operating System(s)	HP-UX
Residing Facility	Pelican Data Center
Exclusion(s) 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 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	SLC	UT	United States of America
Headquarters and Manufacturing	Office	No	N/A	Las Vegas	NV	United States of America
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 e1 assessment. Per HITRUST's Assurance Program Requirements requires the inclusive method must be used on HITRUST e1 validated assessments.

Organizations undergoing e1 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 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 e1 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
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
- Incident management
- Identity and access management
- Compliance management
- Security training and awareness

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 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).

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: 05/27/2022 Report Period: 10/1/2021 – 4/30/2022	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 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.

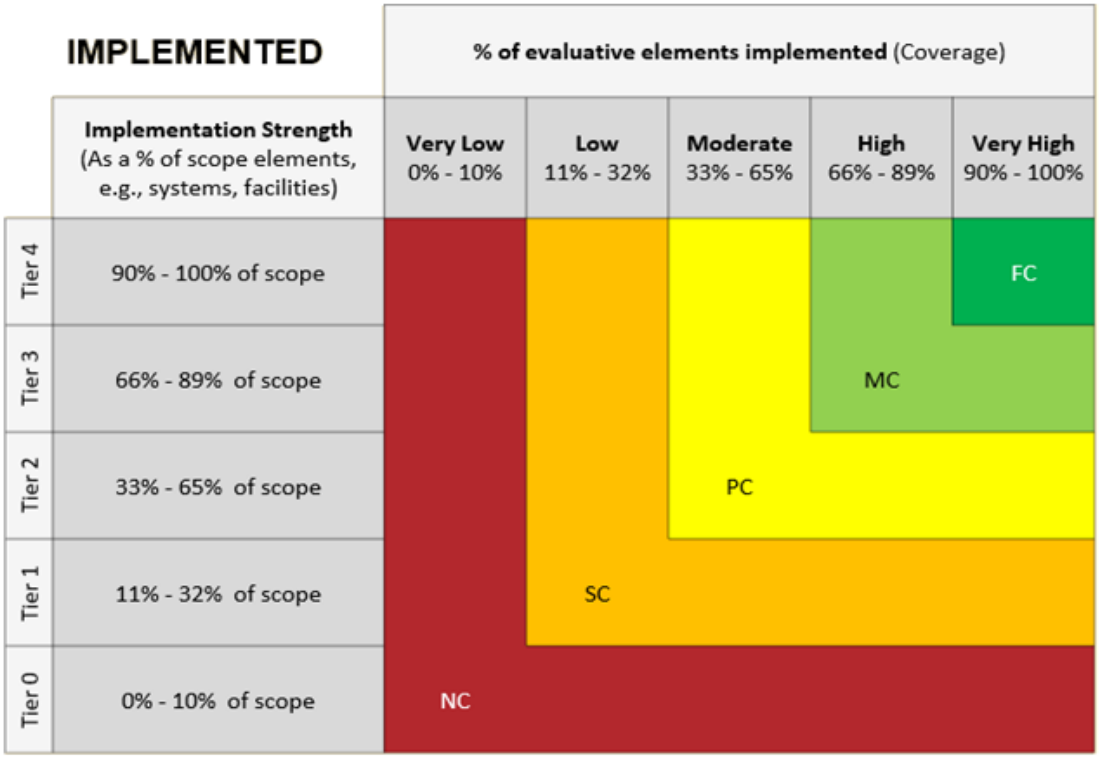
HITRUST developed a scoring rubric that is used by external assessors to determine implementation scoring in a consistent and repeatable way by evaluating both implementation strength and implementation coverage, described as follows:

- 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 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

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.

8. Results by Control Reference

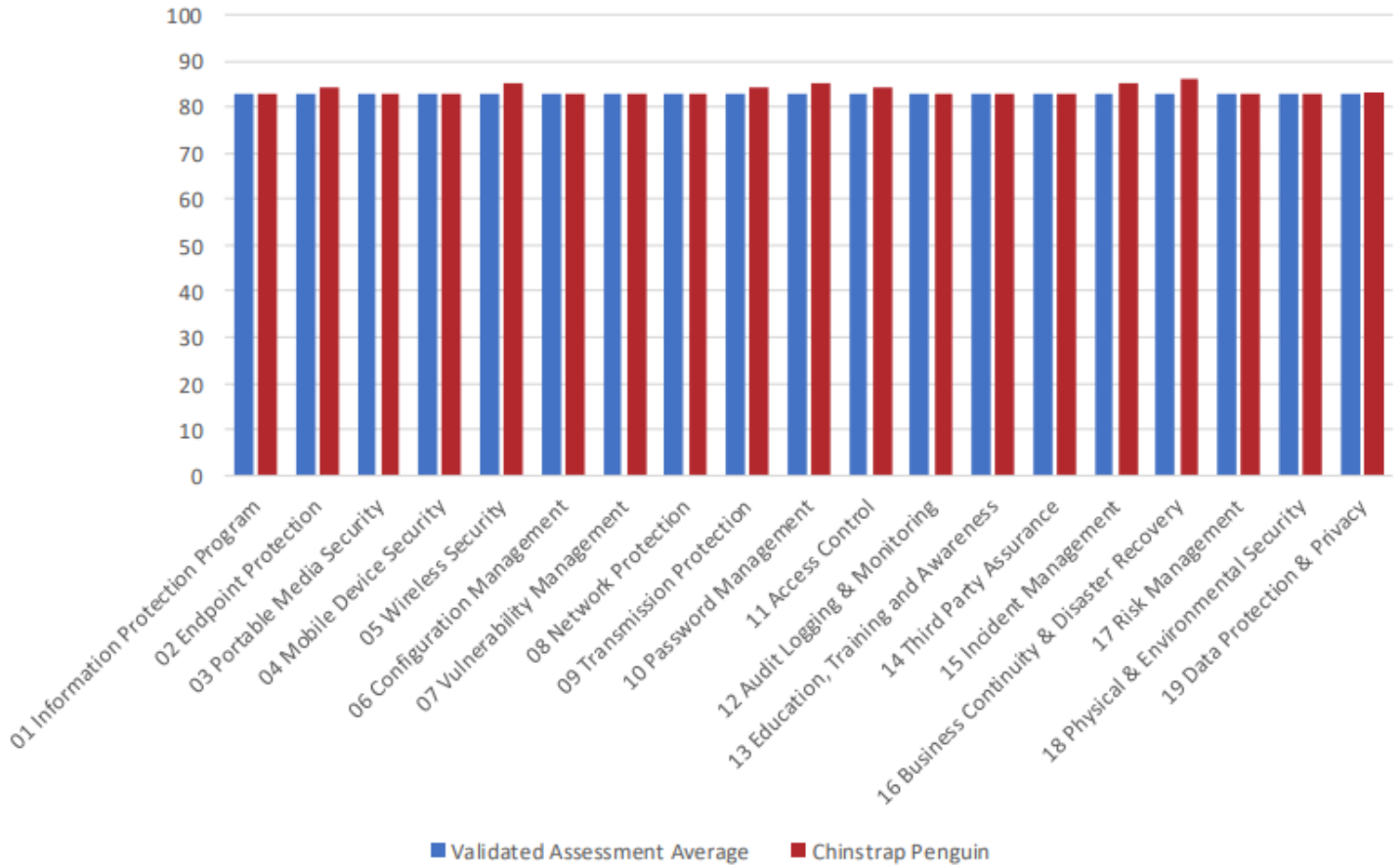
Each HITRUST CSF requirement is associated with a HITRUST CSF control reference. The following table is a control reference-level summary of the results for this assessment.

Control Reference	Maturity Score of 80 or Higher	Requirement with Corrective Action Plan (CAP)	CAP Identifier
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.l Remote Diagnostic and Configuration Port Protection	Yes	None	N/A
01.m Segregation in Networks	Yes	None	N/A
01.p Secure Log-on Procedures	Yes	None	N/A
01.q User Identification and Authentication	Yes	None	N/A
01.t Session Time-Out	Yes	None	N/A
01.x Mobile Computing and Communications	Yes	None	N/A
02.e Information Security Awareness, Education, and Training	Yes	None	N/A
02.i Removal of Access Rights	Yes	None	N/A
03.b Performing Risk Assessments	Yes	None	N/A
04.a Information Security Policy Document	Yes	None	N/A
05.i Identification of Risks Related to External Parties	Yes	None	N/A
07.a Inventory of Assets	Yes	None	N/A

Control Reference	Maturity Score of 80 or Higher	Requirement with Corrective Action Plan (CAP)	CAP Identifier
08.b Physical Entry Controls	Yes	None	N/A
09.aa Audit Logging	Yes	None	N/A
09.ac Protection of Log Information	Yes	None	N/A
09.b Change Management	Yes	None	N/A
09.j Controls Against Malicious Code	Yes	None	N/A
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.o Management of Removable Media	Yes	None	N/A
09.p Disposal of Media	Yes	None	N/A
09.v Electronic Messaging	Yes	None	N/A
09.z Publicly Available Information	Yes	None	N/A
10.h Control of Operational Software	Yes	None	N/A
10.m Control of Technical Vulnerabilities	Yes	None	N/A
11.c Responsibilities and Procedures	Yes	None	N/A

9. Results by Assessment Domain

An organization must achieve a straight average score of at least 83 for each assessment domain to qualify for HITRUST Essentials, 1-year (e1) certification. The chart below presents this assessment's domain averages alongside the domains averages from all Essentials, 1-year (e1) validated assessments submitted to HITRUST.



Assessment Domain	Maturity Score	Fully Implemented HITRUST CSF Requirements
01 Information Protection Program	100	The organization's information security policy is developed, published, disseminated, and implemented. The information security policy documents: state the purpose and scope of the policy; communicate management's commitment; describe management and workforce members' roles and responsibilities; and establish the organization's approach to managing information security.
02 Endpoint Protection	100	The organization implements and regularly updates mobile code protection, including anti-virus and anti-spyware. The organization applies a default-deny rule that drops all traffic via host-based firewalls or port filtering tools on its endpoints (workstations, servers, etc.), except those services and ports that are explicitly allowed.
03 Portable Media Security	100	The organization restricts the use of writable, removable media and personally owned, removable media in organizational systems.
04 Mobile Device Security	100	The organization identifies and encrypts mobile devices and mobile computing platforms that process, store, or transmit sensitive information.
05 Wireless Security	100	The organization ensures wireless access is explicitly approved and wireless access points and devices have appropriate (e. g. , minimum of AES WPA2) encryption enabled for authentication and transmission.

Section 9 has been truncated for this sample report.

Appendix A - Corrective Action Plans Identified

HITRUST requires assessed entities to define corrective action plans (CAPs) for all HITRUST CSF requirements meeting the following criteria: the requirement's overall score is less than 100 (fully compliant) and the associated control reference (e.g., 00.a) averages less than 80. This section lists the CAPs needed to obtain or maintain HITRUST Essentials, 1-year (e1) certification.

None identified

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.

None identified

Appendix C - Assessment Results

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

01 Information Protection Program

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

02 Endpoint Protection

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

Related CSF Control	09.m Network Controls
HITRUST CSF Requirement Statement	The organization applies a default-deny rule that drops all traffic via host-based firewalls or port filtering tools on its endpoints (workstations, servers, etc.), except those services and ports that are explicitly allowed.
Implemented Score	100

03 Portable Media Security

Related CSF Control	09.o Management of Removable Media
HITRUST CSF Requirement Statement	The organization restricts the use of writable, removable media and personally owned, removable media in organizational systems.
Implemented Score	100

04 Mobile Device Security

Related CSF Control	01.x Mobile Computing and Communications
HITRUST CSF Requirement Statement	The organization identifies and encrypts mobile devices and mobile computing platforms that process, store, or transmit sensitive information.
Implemented Score	100

05 Wireless Security

Related CSF Control	09.m Network Controls
HITRUST CSF Requirement Statement	The organization ensures wireless access is explicitly approved and wireless access points and devices have appropriate (e.g., minimum of AES WPA2) encryption enabled for authentication and transmission.
Implemented Score	100

Appendix C has been truncated for this sample report.