HITRUST

NIST Cybersecurity Framework v2.0

Certification Report

Chinstrap Penguin Corporation

Valid for the period
December 22, 2024 - December 22, 2026

SAMPLE FOR ILLUSTRATIVE USE ONLY

HITRUST

Contents

HITRUST 6175 Main Street
Suite 400
Frisco, TX 75034

1. Letter of NIST Cybersecurity Framework v2.0 Certification

December 22, 2024

Chinstrap Penguin Corporation
123 Main Street
Anytown, TX 12345

Based on the results of a HITRUST® Risk-based, 2-year (r2) validated assessment performed by an Authorized External Assessor and documented in a HITRUST r2 validated assessment Report ("Report"), Chinstrap Penguin Corporation (the "Organization") has, for the scope of this assessment ("Scope"), implemented an information protection program that is consistent with the objectives specified in the NIST Cybersecurity Framework (CSF) v2.0.

Scope

The following platforms of the Organization were included within the Scope, which included a review of the referenced facilities and supporting infrastructure within the applicable information protection requirements:

Platform:

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

Facilities:

- CP Framingham Manufacturing Facility (Other) managed internally located in Framingham, Massachusetts, United States of America
- CP Headquarters and Manufacturing (Other) managed internally located in Las Vegas, Nevada, United States of America
- Pelican Data Center (Data Center) managed by Pelican Hosting located in Salt Lake City, Utah, United States of America

Certification

The Organization has met the criteria specified as part of the HITRUST Assurance Program to obtain a HITRUST NIST CSF Report with Certification ("Certification") for the Scope. The Organization obtained a HITRUST r2 Certification, where the certification is awarded based on each domain's average maturity score meeting a minimum threshold score. Within each domain, all the requirement statements maturity scores are validated by an External Assessor and further quality assurance procedures completed by HITRUST.

For the HITRUST NIST CSF assessment HITRUST then determined that:

- The HITRUST CSF controls specified by the Entity's organizational, system and regulatory risk factors were successfully mapped to the NIST Cybersecurity Framework Core Categories.

- The maturity of the Entity's implemented HITRUST CSF controls, as validated by an Authorized External Assessor and reflected in the HITRUST Scorecard for the NIST Cybersecurity Framework, provides a fair representation of the identified controls within each Core Category and its respective subcategories.

- The aggregated maturity scores for each NIST CSF Core Category meet HITRUST's criteria for certification of the Scope addressed by the assessment.

This certification is valid for as long as the Entity's associated HITRUST r2 Certification remains valid but shall not exceed a period of two years from the date of this letter.

A full copy of the HITRUST r2 Certification Report has been issued to the organization listed above. The full Report contains detailed information relating to the effectiveness of information protection controls as defined by the scoping factors selected by management. It also includes further details on the scope of the assessment, testing results, a benchmarks comparing the Organization's results to industry results, details on corrective action plans identified if applicable, and the completed questionnaire. Such detailed information can best be leveraged by individuals/organizations who are familiar with and understand the services provided by the organization listed above.

The Organization's Responsibilities and Assertions

Management of the Organization has provided the following assertions to HITRUST:

- The Organization has acknowledged that, as members of management, they are responsible for the information protection controls implemented as required by the HITRUST.

- The Organization has implemented the information protection controls as described within their assessment.

- The Organization maintains the information security management program via monitoring, review, and periodic re-assessments of the information protection controls.

- The Organization has responded honestly, accurately, and completely to inquiries made throughout the assessment process and certification lifecycle.

- The Organization has provided the External Assessor with accurate and complete records and necessary documentation related to the information protection controls

included within the scope of its assessment.

- The Organization has disclosed all design and operating deficiencies in its information protection controls of which is it aware throughout the assessment process, including those where it believes the cost of corrective action may exceed the benefits.

- No events or transactions have occurred or are pending that would have an effect on the assessment that was performed and used as a basis by HITRUST for issuing the report.

- There have been no communications from regulatory agencies concerning noncompliance with or deficiencies regarding the information protection controls that are included within the Scope of this assessment.

External Assessor Responsibilities

External Assessors are authorized by HITRUST based upon a thorough vetting process to demonstrate their ability to perform HITRUST CSF Assessments, and individual practitioners are required to maintain appropriate credentials based upon their role on HITRUST assessments. Within a HITRUST assessment the External Assessor is responsible for:

- Reviewing and gaining a detailed understanding of the information provided by the Organization.

- Performing sufficient procedures to validate the control maturity scores provided by the Organization.

- Meeting all HITRUST Assessment criteria described within the HITRUST Assessment Handbook.

HITRUST's Responsibilities

HITRUST is responsible for maintenance of the HITRUST CSF, including mapping the NIST CSF Core Categories to HITRUST CSF requirement statements, and HITRUST Assurance Program against which the Organization and an External Assessor completed this assessment.

HITRUST performed a quality assurance review of this assessment to support that the control maturity scores were consistent with the results of testing performed by the External Assessor. HITRUST's quality assurance review incorporated a risk-based approach to substantiate the External Assessor's procedures were performed in accordance with the requirements of the HITRUST Assurance Program.

Additional information on the HITRUST Assurance Program used to support HITRUST's certification of the NIST CSF can be found on the HITRUST website: *https://hitrustalliance.net.*

Limitations of Assurance

Relying parties should consider the following in their evaluation of this report:

- This NIST CSF Certification Report accompanies a HITRUST CSF r2 validated assessment. The accompanying r2 validated assessment was scoped and performed in accordance with the HITRUST Assurance Program requirements designed to measure and report on control maturity for purposes of issuing HITRUST validated assessment reports. Consequently:
    - HITRUST assessments are scoped based on a defined boundary inclusive of specified physical facilities and IT platforms. Therefore, the HITRUST assessment may be scoped differently than an assessment focused exclusively on evaluating NIST CSF controls across the entirety of the Organization.
    - The nature, timing, and extent of the procedures performed by the HITRUST External Assessor Organization may differ from those performed in an assessment dedicated exclusively to evaluating NIST CSF compliance and were not designed to detect all instances of NIST CSF non-compliance specifically.
    - Deficiencies noted in this report, if any, were identified through an evaluation of control maturity of the HITRUST CSF requirements mapping to NIST CSF included in the Organization's HITRUST r2 validated assessment and not in observance of any other criteria specific to NIST CSF requirements.
- Mappings produced by HITRUST to authoritative sources are performed utilizing the NIST OLIR Program methodology outlined in NISTIR 8278 and subjected to HITRUST's internal quality review process.
- No assessment of controls or compliance status provides total assurance or 100% protection against possible control failures and instances of non-compliance. Because of their nature, controls may not prevent, or detect and correct, all errors or omissions relevant to compliance with regulatory statutes.

HITRUST

2. Assessment Context

The NIST Cybersecurity Framework

The NIST Cybersecurity Framework complements rather than replaces an organization's existing risk management process and cybersecurity program by providing an overarching set of guidelines to provide a minimal level of consistency as well as depth, breadth, and rigor of industry's cybersecurity programs, as shown in Figure 1.

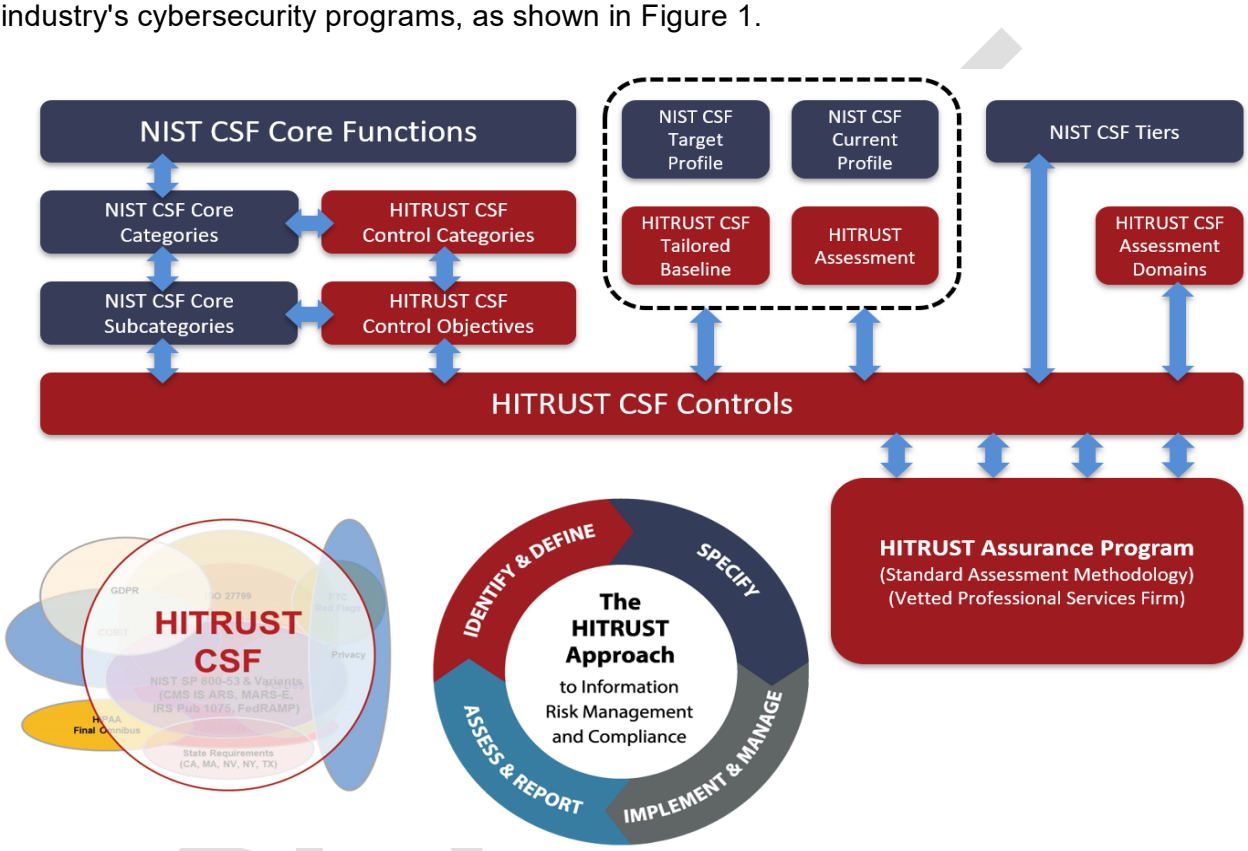

Figure 1. Implementing the NIST Cybersecurity Framework through the HITRUST CSF and CSF Assurance Program

The NIST CSF v2.0 Core is essentially a set of cybersecurity activities, desired outcomes, and applicable references that are common across government and industry. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across an organization from the executive level to the implementation/operations level, from one organization to another, and from one industry to another.

NIST Cybersecurity Framework Core Functions provide an incident response and recovery-oriented view of an organization's cybersecurity needs; the NIST Cybersecurity Framework Core Categories provide topical groupings of cybersecurity activities related to each of the Core Functions; and the NIST Cybersecurity Framework Core Subcategories provide the specific outcomes intended for each Core Category.

Coverage and Reportability

For specific HITRUST CSF control requirements mapping to NIST CSF v2.0 Core Categories, the Organization's HITRUST Risk-based, 2-year (r2) Validated Assessment provided information about how well they had been implemented and the nature and volume of identified gaps in implementation (if any).

The following factors collectively determined the degree of NIST CSF v2.0 coverage and reportability in the Organization's HITRUST assessment:

- HITRUST's approach to incorporating NIST CSF v2.0 Core Categories.
- The Organization's HITRUST CSF assessment preferences and tailoring.

The NIST CSF includes the following three components:

- CSF Core: The taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks. The CSF Core components are a hierarchy of Functions, Categories, and Subcategories that detail each outcome.
- CSF Organizational Profiles: That describe an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes.
- CSF Tiers: These are applied to CSF Organizational Profiles to characterize the rigor of an organization's cybersecurity risk governance and management practices. Additional provide context on how an organization views cybersecurity risks and the processes in place to manage those risks.
- The HITRUST NIST CSF Certification does not provide specific coverage for CSF Organizational Profiles or CSF Tiers. Instead, the HITRUST NIST CSF Certification as well as the HITRUST CSF-to-NIST CSF mappings maintained by HITRUST focus on and provide full coverage for the CSF Core.

Figure 2. NIST CSF Functions

The CSF Core comprises of the five Functions outlined within figure 2 above. These Core Functions provide an incident response and recovery-oriented view of an organization's cybersecurity needs; the NIST CSF Core Categories provide topical groupings of cybersecurity activities related to each of the Core Functions; and the CSF Core Subcategories provide the specific outcomes intended for each Core Category. Each CSF Core Subcategory is mapped to one or more HITRUST CSF requirement statements.

Assessment Approach

An *Authorized HITRUST External Assessor Organization* (the "External Assessor") performed validation procedures to measure the control maturity 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 elsewhere in 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.

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

Implementation Score	Description	Points Awarded
Partially compliant (PC)	About half of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 50% (point estimate) or 33% to 65% (interval estimate).	50
Mostly compliant (MC)	Many but not all of the evaluative elements in HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 75% (point estimate) or 66% to 89% (interval estimate).	75
Fully compliant (FC)	Most if not all of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 100% (point estimate) or 90% to 100% (interval estimate).	100

Risk Factors

The assessed entity completed the following tailoring questionnaire to derive this assessment's customized set of HITRUST CSF requirements based on organizational, technical, and regulatory risk factors.

Assessment Type	
HITRUST Risk-based, 2-year (r2) Security Assessment	
General Risk Factors	
Organization Type	Service Provider (Information Technology, IT)
Entity Type	Healthcare - Business Associate
Do you offer Infrastructure as a Service (IaaS)?	No
Geographic Risk Factors	
Geographic Scope of Operations Considered	Multi-State
Organizational Risk Factors	
Number of Records that are currently held	Between 10 and 60 Million Records
Technical Risk Factors	
Is the system(s) accessible from the Internet?	Yes

Is the scoped system(s) (on-premise or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)?	No – The systems are only accessible by internal resources. Data is not shared and there is no direct third-party access.
Does the system(s) transmit or receive data with a third-party?	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
Is the system(s) publicly positioned?	No - The system is not publicly positioned
Number of interfaces to other systems	25 to 75
Number of users of the system(s)	Fewer than 500
Number of transactions per day	6,750 to 85,000
Does the scoped environment allow dial-up/dial-in capabilities (i.e., functional analog modems)?	No - There are no modems in the solution
Is scoped information sent and/or received via fax machine (i.e., an actual machine, excluding efax or scan to email)?	No - No fax machines used in the environment
Do any of the organization's personnel travel to locations the organization deems to be of significant risk?	No - No Chinstrap personnel travel to locations deemed to be of significant risk.
Are hardware tokens used as an authentication method within the scoped environment?	No - There are no hardware tokens in use.
Does the organization allow personally owned devices to connect to scoped organizational assets (i.e., BYOD - bring your own device)?	Yes
Are wireless access points in place at any of the organization's in-scope facilities?	No - There are no wireless access points in the environment.
Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component?	No - There is no in-house or outsourced information systems development.
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 - There are no electronic signatures in use.
Is scoped information sent by the organization using courier services, internal mail services, or external mail services (e.g., USPS)?	Yes
Is any aspect of the scoped environment hosted on the cloud?	No – No aspect of the scoped environment is hosted on the cloud

Does the system allow users to access the scoped environment from an external network that is not controlled by the organization?	Yes

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

HITRUST

3. Scope of the Assessment

Company Background

Chinstrap Penguin Corp is a manufacturer, retailer and distributor of widgets for use in the care, feeding and housing of all Antarctic Chinstrap Penguins. Chinstrap Penguin Corp was established in 2005 and has grown to one of the largest widget producers in the world and now offers a number of specialized widgets to its customers and third-party distributors. In 2014 Chinstrap Penguin Corp entered the gadget market by acquiring Gadget Group and is now the third largest gadget manufacturer in the United States.

In-scope Platform

The following table describes the platform that was included in the scope of this assessment.

Customer Central (a.k.a. "Portal")	
Description	The Portal is a platform that allows numerous applications and service offerings to be accessed by customers via a single web-based interface via a browser. It does this for numerous customers and allows their customers to obtain information in a single location. Chinstrap Penguin personnel access the Portal through a secure VPN to a bastion host. From the bastion host systems administrators connect via VDI to an administrative console for management of all in-scope applications and supporting infrastructure. The Portal is developed by Chinstrap Penguin personnel. It is built in Java and .Net. The solution leverages VMWare for scalability. The applications/service offerings that make up the Portal are Penguin Nest, Penguin Analytics, and South Pole Benefit Eligibility. • Penguin Nest is an application that delivers content and applications from customer systems via the Portal. The application collects and feeds critical metrics to Penguin Analytics. • Penguin Analytics is an application that delivers reporting and analytics capability to customers. It allows them to develop dashboards and reports and track KPIs with their information that is stored within the Portal. • South Pole Benefits Eligibility allows our customers to provide benefit eligibility information so that users of the system have a single place to go to get the eligibility information from multiple customers. Meta data from the application is fed to Penguin Analytics for further analysis by customer
Application(s)	Penguin Nest, Penguin Analytics, South Pole Benefits Eligibility

Database Type(s)	Oracle
Operating System(s)	HP-UX
Residing Facilities	Pelican Data Center

In-scope Facilities

The following table presents the facilities that were included in the scope of this assessment.

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

Services Outsourced

The following table presents outsourced services relevant to the scope of this assessment. The “Consideration in this Assessment” column of 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. Confidential Page 11 of 27 © 2021 HITRUST Alliance Chinstrap Penguin Corp HITRUSTAlliance.net

Organizations undergoing i1 validated assessments have two options of how to address situations in which a HITRUST CSF requir ement 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

4. 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).

Third-party Report Type	Assessed Entity	Assessment Type	Utilization Approach	Relevant Platforms	Relevant Facilities	Assessment Domains
Pelican Hosting SOC2 Type II	Pelican Hosting	Period-of-Time assessment report (e.g. SOC2 Type II)	Issuance Date: 05/27/2024	Customer Central (a.k.a. “Portal”)	Pelican Data Center	18 Physical & Environmental Security

HITRUST

5. Summary Assessment Results

HITRUST's certification of the Organization's NIST CSF implementation is based on the NIST Cybersecurity Framework v2.0 Core and as summarized in the scorecard below. This scorecard reflects the aggregated scores for the underlying HITRUST CSF requirements as they are mapped by HITRUST to the NIST Cybersecurity Framework core functions, categories, and subcategories.

To qualify for HITRUST's NIST CSF certification an organization must achieve a straight average score of at least 70 for each NIST CSF function and category. The table below presents the control maturity scoring averages of all NIST CSF functions and categories included in this assessment alongside the function and category scoring averages across all r2 submitted to HITRUST (labeled as "Avg. HITRUST r2 score").

Govern

NIST CSF Core item	Average score in this assessment	Certification scoring threshold of 70 achieved?
GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored	78.35 / 100.00 Avg. HITRUST r2 score: 74.71	Yes
Organizational Context (GV.OC): The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood	82.29 / 100.00 Avg. HITRUST r2 score: 74.02	Yes
GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	84.38 / 100.00 Avg. HITRUST r2 score: 77.63	-
GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	81.25 / 100.00 Avg. HITRUST r2 score: 77.47	-
GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed	81.97 / 100.00 Avg. HITRUST r2 score: 73.03	-

NIST CSF Core item	Average score in this assessment	Certification scoring threshold of 70 achieved?
GV.OC-04: Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated	85.94 / 100.00 Avg. HITRUST r2 score: 75.79	-
GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated	84.38 / 100.00 Avg. HITRUST r2 score: 75.38	-
Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions	78.25 / 100.00 Avg. HITRUST r2 score: 74.79	Yes
GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders	81.25 / 100.00 Avg. HITRUST r2 score: 74.09	-
GV.RM-02: Risk appetite and risk tolerance statements are established, communicated, and maintained	81.25 / 100.00 Avg. HITRUST r2 score: 75.14	-
GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes	81.25 / 100.00 Avg. HITRUST r2 score: 73.22	-
GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated	81.25 / 100.00 Avg. HITRUST r2 score: 76.05	-

Section 4 has been truncated for this sample report.

HITRUST

Appendix A. Relevant Observations

During the HITRUST r2 assessment which led to in this NIST CSF report, the policy, procedure, and/or implemented control maturity level(s) on each of the following HITRUST CSF requirements scored less than "Fully Compliant". These conditions were identified as relevant to the Organization's NIST CSF implementation, as each of these HITRUST CSF requirements map to one or more NIST CSF v2.0 subcategories. Those relying on this report should evaluate these items (and the associated risk treatment) in consultation with the Organization.

NIST CSF subcategory	Mapped HITRUST CSF requirement	Maturity level(s) scoring less than fully compliant	Corrective Action(s) [Unvalidated]
GV.SC-02	**Mapped BUID: 0151.02c1Organizational.23 / CVID: 0316.0** . The organization ensures that employees, contractors, and third-party users agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to the organization's assets associated with information systems and services. The organization develops and documents access agreements for organizational systems. Privileges are not granted until the terms and conditions have been satisfied and agreements have been signed.	Policy, Procedure, Implemented	[Status: Started - On Track, Target Date: 3/14/2025] The organization will update policies and procedures to require access agreements for each organizational system. The organization will ensure that privileges are not granted before access agreements are signed.

Appendix A has been truncated for this sample report.

HITRUST

Appendix B. Relevant Assessment Results and Mappings

Below are the assessment results and control maturity evaluations for each assessed HITRUST CSF requirement mapped to the NIST Cybersecurity Framework v2.0.

In addition to relevant assessment results and control maturity evaluations, the table below lists the HITRUST CSF requirements mapped by HITRUST to each NIST Cybersecurity Framework (CSF) v2.0 subcategory. Note that many more mappings exist between the NIST CSF and the HITRUST CSF; this section lists only the mapping subset relevant to the underlying HITRUST assessment as determined through the factors described in the Assessment Context section of this report.

The HITRUST CSF is mapped to dozens of other authoritative sources in addition to the NIST CSF, enabling a wide range of compliance coverage within HITRUST Assessments. Mappings produced by HITRUST are performed utilizing the NIST OLIR Program methodology outlined in NIST Interagency Report 8278. These mappings were created by HITRUST and have undergone HITRUST's internal quality review process consisting of at least five of review before being finalized: automated review, initial mapper review, peer review, management review, and quality assurance review. Questions about these mappings should be routed to HITRUST's Support team.

Govern

HITRUST CSF Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring	Measured Scoring	Managed Scoring
Organizational Context (GV.OC): The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood					
GV.OC-01: The organizational mission is understood and informs cybersecurity risk management					

HITRUST CSF Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring	Measured Scoring	Managed Scoring
BUID: 0101.00a1Organizational.123 / CVID: 0001.0 . The organization has a formal information security management program (ISMP) that is documented and addresses the overall security program of the organization. Management support for the ISMP is demonstrated through signed acceptance or approval by management. The ISMP is based on an accepted industry framework, considers all the control objectives of the accepted industry framework, documents any excluded control objectives of the accepted industry framework and the reasons for their exclusion, and is updated at least annually or when there are significant changes in the environment.	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)
BUID: 0113.04a1Organizational.2 / CVID: 0431.1 . 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.	MC: Mostly Compliant (75%)	MC: Mostly Compliant (75%)	MC: Mostly Compliant (75%)	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)

BUID: 0113.04a2Organizational.1 / CVID: 0431.2. As applicable to the focus of a security policy particular document, security policies contain: the organization's mission, vision, values, objectives, activities, and purpose, including the organization's place in critical infrastructure; a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing; a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives; a framework for setting control objectives and controls, including the structure of risk assessment and risk management; the need for information security; the goals of information security; the organization's compliance scope; legislative, regulatory, and contractual requirements, including those for the protection of covered information and the legal and ethical responsibilities to protect this information; arrangements for notification of information security incidents, including a channel for raising concerns regarding confidentially, without fear of blame or recrimination; a definition of general and specific responsibilities for information security management, including reporting information security incidents; references to documentation which may support the policy (e.g., more detailed security policies and procedures for specific information systems or security rules users comply with); a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization (including but not limited to CSF control objectives such as: (a) compliance with legislative, regulatory, and contractual requirements; (b) security education, training, and awareness requirements for the workforce, including researchers and research participants; (c) incident response and business continuity management; (d) consequences of information security policy violations; (e) continuous monitoring; (f) designating and maintaining an appropriately resourced and technically experienced information security team; (g) physical security of areas where sensitive information (e.g., PII, PCI and PMI data); and (h) coordination among organizational entities. As applicable to the focus of a security policy	MC: Mostly Compliant (75%)	MC: Mostly Compliant (75%)	MC: Mostly Compliant (75%)	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)

HITRUST CSF Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring	Measured Scoring	Managed Scoring
particular document, security policies also prescribe the development, dissemination, and review/update of formal, documented procedures to facilitate the implementation of security policy and associated security controls.					
BUID: 0114.04b1Organizational.1 / CVID: 0435.0 . The information security policy documents are reviewed at planned intervals or if significant changes occur to ensure the policies' continuing adequacy and effectiveness. Security policies are communicated throughout the organization.	MC: Mostly Compliant (75%)	MC: Mostly Compliant (75%)	MC: Mostly Compliant (75%)	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)
BUID: 17.03aISO31000Organizational.5 / CVID: 2822.0 . The organization defines the scope of its risk management activities.	MC: Mostly Compliant (75%)	MC: Mostly Compliant (75%)	MC: Mostly Compliant (75%)	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)

Appendix B has been truncated for this sample report.

Appendix C. HITRUST Background

HITRUST Alliance, Inc. was born out of the belief that information security should be a core pillar of, rather than an obstacle to, the broad adoption of information systems and exchanges. HITRUST®, in collaboration with industry, business, technology and information security leaders, established the HITRUST CSF, a certifiable framework that can be used by any and all organizations that create, access, store or exchange personal, sensitive, and/or financial information.

Beyond the establishment of the HITRUST CSF®, HITRUST is also driving the adoption of and widespread confidence in the framework and sound risk management practices through awareness, education, advocacy, and other outreach activities.

An integral component to achieving HITRUST's goal to advance the protection of sensitive information is the establishment of a practical mechanism for validating an organization's compliance with the HITRUST CSF.

The HITRUST CSF is an overarching security framework that incorporates and leverages the existing security requirements placed upon organizations, including international (GDPR, ISO), federal (e.g., FFIEC, HIPAA and HITECH), state, third party (e.g., PCI and COBIT), and other government agencies (e.g., NIST, FTC, and CMS). The HITRUST CSF is already being widely adopted by leading organizations in a variety of industries as their information protection framework.

HITRUST has developed the HITRUST Assurance Program, which encompasses the common requirements, methodology and tools that enable both an organization and its business partners to take a consistent and incremental approach to managing compliance.

The HITRUST Assurance Program is the mechanism that allows organizations and their business partners and vendors to assess and report against multiple sets of requirements. Unlike other programs, the oversight, vetting, and governance provided by HITRUST and the HITRUST Assessor Council affords greater assurances and security across all industries.

For more information about HITRUST, the HITRUST CSF and other HITRUST offerings and programs, visit *https://hitrustalliance.net.*