



# HITRUST Risk-based, 2-year (r2)

## Certification Report

**Chinstrap Penguin Corp.**

Valid for the period  
December 11, 2025 - December 11, 2027

This report is provided exclusively for internal  
business use by Example Org

Downloaded by john.doe@example.com on 10/1/2026

**SAMPLE REPORT FOR ILLUSTRATIVE USE ONLY**



View this assessment in the  
[HITRUST Report Center](#)



## Contents

|                                                                  |    |
|------------------------------------------------------------------|----|
| 1. Letter of HITRUST Risk-based, 2-year (r2) Certification ..... | 3  |
| 2. Assessment Context .....                                      | 7  |
| About the HITRUST r2 Assessment and Certification .....          | 7  |
| Assessment Approach .....                                        | 7  |
| Risk Factors .....                                               | 9  |
| 3. Scope of the Assessment .....                                 | 11 |
| 4. Use of the Work of Others .....                               | 14 |
| 5. Summary Assessment Results .....                              | 15 |
| 6. Results by Control Reference .....                            | 16 |
| Appendix A - Corrective Action Plans Identified .....            | 17 |
| Appendix B - Additional Gaps Identified .....                    | 18 |
| Appendix C - Assessment Results .....                            | 19 |
| 01 Information Protection Program .....                          | 19 |
| Appendix D - HITRUST Background .....                            | 20 |

For Internal Use by Example Org



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

December 11, 2025

Chinstrap Penguin Corp.  
123 Main Street  
Anytown, Texas 12345

HITRUST has developed the HITRUST CSF, a certifiable security and privacy framework which incorporates information protection requirements based on input from leading organizations. HITRUST identified a subset of the HITRUST CSF requirements that an organization must meet to be HITRUST Risk-based, 2-year (r2) Certified for a defined assessment scope. Chinstrap Penguin Corp. ("the Organization") has chosen to perform a HITRUST CSF v11.4.0 r2 assessment. The assessment was performed utilizing a HITRUST Authorized External Assessor Organization ("External Assessor").

### Scope

The following platform of the Organization was included within the scope of this assessment ("Scope") which included a review of the referenced facilities and supporting infrastructure for the applicable information protection requirements:

Platform:

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

Facilities:

- CP Framingham Manufacturing Facility (Office) located in Framingham, MA, United States of America
- CP Headquarters and Manufacturing (Office) located in Las Vegas, NV, United States of America
- Pelican Data Center (Data Center) managed by Pelican Hosting located in Salt Lake City, UT, United States of America

### Certification

The Organization has met the criteria specified as part of the HITRUST Assurance Program to obtain a HITRUST Risk-based, 2-year (r2) Validated Assessment report with certification ("Certification") for the Scope. Certification is awarded based on each domain's average maturity score meeting a minimum score. Within each domain the maturity scores for each



requirement statement were validated by an External Assessor and the assessment was subjected to quality assurance procedures performed by HITRUST.

The Certification for the Scope is valid for a period of two years from the date of this letter 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 security events resulting in unauthorized access to the assessed environment or data housed therein, including any data security breaches occurring within or affecting the assessed environment reportable to a federal or state agency by law or regulation.
- No significant changes in the business or security policies, practices, controls, and processes have occurred that might impact its ability to meet the HITRUST certification criteria specified as part of the HITRUST Assurance Program.

Users of this letter can contact HITRUST customer support ([support@hitrustalliance.net](mailto:support@hitrustalliance.net)) for questions on using this letter.

### **The Organization's 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 it is 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. In HITRUST r2 validated assessments 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 Responsibilities**

HITRUST is responsible for maintenance of the HITRUST CSF 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 about the HITRUST CSF and HITRUST Assurance Program used to support this assessment can be found on the HITRUST website (<https://hitrustalliance.net>).



### **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. The assessment is not a substitute for a comprehensive risk management program but is a critical data point in risk analysis. The assessment should also not be a substitute for management oversight and decision-making but, again, leveraged as a key input.

### **Distribution and Use Restriction**

This report is provided exclusively for the internal business use of Example Org. Distribution, publication, or disclosure of this report outside of Example Org, in whole or in part, is prohibited. This document contains recipient-specific identifying information and may be monitored for unauthorized distribution.

HITRUST



## 2. Assessment Context

### About the HITRUST r2 Assessment and Certification

The HITRUST r2 assessment provides the highest level of information protection and compliance assurance. It is the most comprehensive and robust HITRUST certification, and can be optionally tailored to include coverage for additional authoritative sources such as HIPAA, the NIST Cybersecurity Framework, and GDPR.

The HITRUST r2 assessment is an evolving, threat-adaptive assessment with an accompanying certification. HITRUST r2 assessments leverage threat intelligence data and best practice controls to deliver an assessment that addresses relevant practices and active cyber threats. To do this, HITRUST continually evaluates cybersecurity controls to identify those relevant to mitigating known risks using cyber threat intelligence data from leading threat intelligence providers. Therefore, the HITRUST r2 includes controls that exclusively address emerging cyber threats actively being targeted today.

### Assessment Approach

The External Assessor performed validation procedures based upon the scope of the assessment and in observance of the requirements in the HITRUST Assessment Handbook. Validation procedures 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.

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 r2 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 Compliant (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            |

For Internal



## Risk Factors

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

### Assessment Type

HITRUST Risk-based, 2-year (r2)

### General Risk Factors

|                                                       |                                                   |
|-------------------------------------------------------|---------------------------------------------------|
| Entity type designation in the US healthcare industry | US Healthcare - Business Associate                |
| Are you a Group Health Plan?                          | No - The organization is not a group health plan. |
| Do you offer Infrastructure as a Service (IaaS)?      | No                                                |
| Organization Type                                     | Service Provider (Information Technology, IT)     |

### Technical Risk Factors

|                                                                                                                                                                                                                                                                                                 |                                                                          |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| Does the organization allow personally owned devices to connect to scoped organizational assets (i.e., BYOD - bring your own device)?                                                                                                                                                           | Yes                                                                      |
| Is any aspect of the scoped environment hosted on the cloud?                                                                                                                                                                                                                                    | No - No aspect of the scoped environment is hosted on the cloud          |
| Is scoped information sent by the organization using courier services, internal mail services, or external mail services (e.g., USPS)?                                                                                                                                                          | Yes                                                                      |
| 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 scoped environment allow dial-up/dial-in capabilities (i.e., functional analog modems)?                                                                                                                                                                                                | No - There are no modems in the solution                                 |
| 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.                          |
| Does the system allow users to access the scoped environment from an external network that is not controlled by the organization?                                                                                                                                                               | Yes                                                                      |
| 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                             |

|                                                                                                                                                      |                                                                                                                                                   |
|------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Does the organization use any part of the scoped systems, system components, or system services to sell goods and/or services?</b>                | Yes                                                                                                                                               |
| <b>Is the system(s) accessible from the Internet?</b>                                                                                                | Yes                                                                                                                                               |
| <b>Number of interfaces to other systems</b>                                                                                                         | 25 to 75                                                                                                                                          |
| <b>Number of transactions per day</b>                                                                                                                | 6,750 to 85,000                                                                                                                                   |
| <b>Number of users of the system(s)</b>                                                                                                              | Fewer than 500                                                                                                                                    |
| <b>Is the system(s) publicly positioned?</b>                                                                                                         | No - The system is not publicly positioned                                                                                                        |
| <b>Is the scoped system(s) (on-premises or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)?</b> | No - The systems are only accessible by internal resources. Data is not shared and there is no direct third-party access.                         |
| <b>Does the system(s) transmit or receive data with a third-party?</b>                                                                               | 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 |
| <b>Are hardware tokens used as an authentication method within the scoped environment?</b>                                                           | No - There are no hardware tokens in use.                                                                                                         |
| <b>Do any of the organization's personnel travel to locations the organization deems to be of significant risk?</b>                                  | No - No Chinstrap personnel travel to locations deemed to be of significant risk                                                                  |
| <b>Are wireless access points in place at any of the organization's in-scope facilities?</b>                                                         | No - There are no wireless access points in the environment.                                                                                      |

## Compliance Factors (Optional)

For Internal Use

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

| Customer Central (a.k.a. "Portal") |                     |
|------------------------------------|---------------------|
| Residing Facility                  | Pelican Data Center |
| Exclusion(s) from scope            | None                |

## 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                  |
|--------------------------------------|------------------|----------------------|----------------------|----------------|-------|--------------------------|
| CP Framingham Manufacturing Facility | Office           | No                   | -                    | Framingham     | MA    | United States of America |
| CP Headquarters and Manufacturing    | Office           | No                   | -                    | Las Vegas      | NV    | United States of America |
| Pelican Data Center                  | Data Center      | Yes                  | Pelican Hosting      | Salt Lake City | UT    | 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 r2 assessment. HITRUST requires the inclusive method must be used on HITRUST r2 validated assessments. Under the Inclusive method, 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.

| Third-party Provider | Relevant Service(s) Provided                                                                                                                                             | Consideration in this Assessment |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| Pelican Hosting      | Pelican Hosting provides a colocation facility where Chinstrap maintains a dedicated cage. Pelican Hosting personnel do not have logical access to any in-scope systems. | Included                         |

For Internal Use by Example Org

## 4. Use of the Work of Others

For certain portions of the assessment and as allowed by HITRUST's Assurance Program requirements within the Assessment Handbook, the external assessor may have utilized the work of other assessors, auditors, and/or inspectors in lieu of direct testing. All assessment Use of the Work of Others, 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).

Work of other assessors was not relied upon in the HITRUST CSF assessment underlying this report (i.e., no inheritance or third-party reliance was utilized).



## 5. Summary Assessment Results

An organization must achieve a straight average score of at least 62 for each assessment domain to qualify for HITRUST Risk-based, 2-year (r2) certification.

The table below presents the control maturity scoring averages of all assessment domains included in this assessment alongside the domain scoring averages across all r2 validated assessments submitted to HITRUST (labeled as "Avg. HITRUST r2 score", including Measured and Managed maturity level scores). Note that the Organization that excludes the measured and managed maturity levels from consideration of this assessment makes 75.00 the highest maturity score directly achievable instead of 100.00

| Assessment Domain                 | Policy maturity average score in this assessment | Procedure maturity average score in this assessment | Implemented maturity average score in this assessment | Average domain score of this assessment              | Certification scoring threshold of 62 achieved? |
|-----------------------------------|--------------------------------------------------|-----------------------------------------------------|-------------------------------------------------------|------------------------------------------------------|-------------------------------------------------|
| 01 Information Protection Program | 15.00 / 15.00 points                             | 17.67 / 20.00 points                                | 40.00 / 40.00 points                                  | 72.67 / 75.00 points<br>Avg. HITRUST r2 score: 75.22 | Yes                                             |
| 02 Endpoint Protection            | 15.00 / 15.00 points                             | 20.00 / 20.00 points                                | 40.00 / 40.00 points                                  | 75.00 / 75.00 points<br>Avg. HITRUST r2 score: 75.72 | Yes                                             |

*This section has been truncated for this sample report*

## 6. 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.

The table below presents the control maturity scoring averages of all HITRUST CSF control references included in this assessment alongside the control reference scoring averages across all r2 validated assessments submitted to HITRUST (labeled as "Avg. HITRUST r2 score", including Measured and Managed maturity level scores). Note that the Organization that excludes the measured and managed maturity levels from consideration of this assessment makes 75.00 the highest maturity score directly achievable instead of 100.00

Note that the Organization chose to exclude the measured and managed maturity levels from consideration in this assessment, making 75.00 (instead of 100.00) the highest maturity score directly achievable.

| Control Reference<br>(* indicates required for r2 cert.) | Control Specification                                                                                                                                                                              | Requirement Statements | Control ref. average maturity score           | Control ref. average maturity score of 71 achieved? |
|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|-----------------------------------------------|-----------------------------------------------------|
| 00.a Information Security Management Program*            | An Information Security Management Program (ISMP) shall be defined in terms of the characteristics of the business, and established and managed including monitoring, maintenance and improvement. | 6 applicable           | 71.67 / 75.00<br>Avg. HITRUST r2 score: 75.31 | Yes                                                 |
| 01.a Access Control Policy                               | An access control policy shall be established, documented, and reviewed based on business and security requirements for access.                                                                    | 2 applicable           | 75.00 / 75.00<br>Avg. HITRUST r2 score: 75.17 | Yes                                                 |

This section 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 71, the requirement's implemented maturity level scores less than "fully compliant", the associated control reference (e.g., 00.a) is required for HITRUST Risk-based, 2-year (r2) certification, and the associated control reference averages less than 71. This section lists the CAPs needed to obtain and maintain HITRUST Risk-based, 2-year (r2) certification.

**None identified**

For Internal Use by Example Org

## Appendix B - Additional Gaps Identified

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

| Requirement                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Control Reference                    | Maturity Score | Maturity Level(s) Deficient |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|----------------|-----------------------------|
| BUID: 0105.02a2Organizational.1 / CVID: 0299.0 . The organization assigns risk designations to all organizational positions as appropriate, establishes screening criteria for risk designations as appropriate, and reviews and revises designations every 365 days.                                                                                                                                                                                                                                                                                                                   | 02.a Roles and Responsibilities      | 65.00          | Process                     |
| BUID: 0666.10h1System.5 / CVID: 1892.0 . The organization maintains an up-to-date list of authorized software that is required in the enterprise for any business purpose on any business system.                                                                                                                                                                                                                                                                                                                                                                                       | 10.h Control of Operational Software | 67.50          | Policy                      |
| BUID: 08.09n2Organizational.8 / CVID: 0943.1 . The organization authorizes connections from the information system to other information systems outside of the organization through the use of interconnection security agreements or other formal agreement. The organization documents for each connection the interface characteristics, the security requirements, and the information communicated. The organization employs a deny-all, permit-by-exception policy for allowing connections from the information system to other information systems outside of the organization. | 09.n Security of Network Services    | 65.00          | Implementation              |

*This section has been truncated for this sample report*



## 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               | 05.a Management Commitment to Information Security                                                                                                                                                                                                                                                                                                    |                                   |                                       |
| HITRUST CSF Requirement Statement | <b>BUID: 0117.05a1Organizational.1   CVID: 0440.0</b> . A senior-level information security official is appointed. The senior-level information security official is responsible for ensuring the organization's information security processes are in place, communicated to all stakeholders, and consider and address organizational requirements. |                                   |                                       |
| Maturity Assessment               | Policy<br>Fully Compliant (100%)                                                                                                                                                                                                                                                                                                                      | Process<br>Fully Compliant (100%) | Implemented<br>Fully Compliant (100%) |

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                   |                                       |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|---------------------------------------|
| Related CSF Control               | 02.d Management Responsibilities                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                   |                                       |
| HITRUST CSF Requirement Statement | <b>BUID: 0112.02d2Organizational.3   CVID: 0331.0</b> . Acceptable usage is explicitly authorized and defined. Defined acceptable usage includes: explicit management approval (authorization) to use the technology; authentication for use of technology; acceptable uses of technologies, with special emphasis on the inappropriate access by workers to personal information of neighbors, colleagues and relatives; acceptable network locations for the technologies; list of company-approved products, including cloud-based services for usage and the storage of company data; activation of modems for vendors only when needed by vendors, with immediate deactivation after use; and prohibition of storage of covered data onto local hard drives, floppy disks, or other external media. |                                   |                                       |
| Maturity Assessment               | Policy<br>Fully Compliant (100%)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Process<br>Fully Compliant (100%) | Implemented<br>Fully Compliant (100%) |

*This section has been truncated for this sample report*



## Appendix D - 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>.