HITRUST

NY OHIP Moderate-Plus Security Baselines v5.0 Insights

Based upon a HITRUST Essentials, 1-year (e1) Validated Assessment

Chinstrap Penguin Corp.

As of August 18, 2025

SAMPLE FOR ILLUSTRATIVE USE ONLY

Contents

Transmittal Letter 3

NY OHIP Scorecard 6

- AC - Access Controls 7
- AT - Awareness Training 9

Scope of the Assessment 10

Use of the Work of Others 13

Limitations of Assurance 14

NY OHIP Overview 15

NY OHIP Coverage and Reportability 16

Appendix A: NY OHIP - Relevant Observations 17

Appendix B: Relevant HITRUST Assessment Results and Mappings 19

- AC - Access Controls 19

Appendix C: HITRUST Background 23

HITRUST

Transmittal Letter

August 18, 2025

Chinstrap Penguin Corp.
123 Main Street
Anytown, TX 12345

Through HITRUST's "Assess Once, Report Many" capability made possible through the HITRUST CSF, HITRUST has prepared this NY OHIP Moderate-Plus Security Baselines v5.0 ("NY OHIP") Insights Report at the request of Chinstrap Penguin Corp ("the Organization"). This Insights Report contains detailed information regarding the coverage and maturity of controls supporting the Organization's compliance with HITRUST CSF requirements mapping to NY OHIP for the scope outlined below, based on a HITRUST Essentials, 1-year (e1) assessment using v11.6.0 of the HITRUST CSF. The Organization can leverage this report to share information regarding their NY OHIP compliance efforts with internal and external stakeholders.

The full e1 validated assessment report contains detailed information relating to the maturity of information protection controls as defined by the tailoring factors selected by management of the Organization. It includes detailed assessment results, a benchmark report comparing the Organization's results to industry results, and details on corrective action plans (if applicable). Such detailed information can best be leveraged by relying parties who are familiar with and understand the services provided by the Organization. Those interested in obtaining a copy of the full report should contact the Organization directly.

Scope

The e1 assessment that this Insights Report is based upon included the following platform, facilities, and supporting infrastructure of the Organization ("Scope"):

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 (Office) located in Salt Lake City, UT, United States of America
- Pelican Data Center (Data Center) managed by Pelican Hosting located in Salt Lake City, UT, United States of America

The Organization's Responsibilities and Assertions

Management of the Organization is responsible for the implementation, operation, and monitoring of the control environment for the Scope. Through execution of this responsibility, and completion of a HITRUST Essentials, 1-year (e1) validated assessment, the Organization asserted that management of the Organization:

- Is responsible for the implementation of information protection controls.
- Disclosed all design and operating deficiencies in their information protection controls which they are aware, including those for which they believe the cost of corrective action may exceed the benefits.
- Is not aware of any events or transactions that have occurred or are pending that would have an effect on the Essentials, 1-year (e1) validated assessment that was performed and used as a basis by HITRUST for issuing that report.
- Is not aware of communications from regulatory agencies concerning noncompliance with or deficiencies regarding the information protection controls that are included within the scope of the assessment.

The NY OHIP Risk Assessment control family requires organizations to conduct a risk assessment and to "update the risk assessment report before issuing a new Authority to Operate (ATO)/authorization or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system or if none of these events occur, update at a minimum every three (3) years". While numerous HITRUST CSF requirements dealing with the Organization's performance of risk analyses are evaluated during HITRUST CSF assessments, HITRUST CSF assessments are not risk assessments. Management of the Organization is responsible for performing and maintaining a risk analysis which adheres to RA-3 of NY OHIP.

Management of the Organization is also solely responsible for ensuring the Organization's compliance with any legal and/or regulatory requirements, including NY OHIP.

External Assessor's 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 on their role in HITRUST assessments. In HITRUST validated assessments, the External Assessor is responsible for the following:

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

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

HITRUST's Responsibilities

HITRUST is responsible for the maintenance of the HITRUST CSF and HITRUST Assurance Program against which the Organization and an Authorized HITRUST External Assessor completed this assessment.

HITRUST is also responsible for producing the mappings from various authoritative sources, including NY OHIP, to the HITRUST CSF. Additional information about HITRUST's 'Assess Once, Report Many' approach and on the HITRUST CSF Assurance Program used to support this compliance assessment can be found on the HITRUST website at https://hitrustalliance.net.

Limitations of Assurance

Parties relying on this report should understand the limitations of assurance specified in the Limitations of Assurance section of this report.

HITRUST

NY OHIP Scorecard

The tables below provide insights on NY OHIP compliance for the environment assessed. Each NY OHIP requirement listed is assigned a compliance score for the implemented control maturity level. The compliance scores are based on the assessment results of the HITRUST CSF requirement(s) as mapped to the NY OHIP requirement. The measured and managed control maturity levels are not included in this scorecard, as these control maturity levels were not assessed in the underlying HITRUST CSF assessment as a result of the Organization's assessment tailoring. These mappings can be found in Appendix B of this document.

To learn about the HITRUST control maturity evaluation and scoring approach, visit https://hitrustalliance.net/content/uploads/Evaluating-Control-Maturity-Using-the-HITRUST-Approach.pdf.

Scorecard Color Legend

PC	Partially Compliant: The control maturity level's scores across all HITRUST CSF requirements included in the Organization's HITRUST assessment mapped to the NY OHIP requirement averaged 33 - 65.99%.
MC	Mostly Compliant: The control maturity level's scores across all HITRUST CSF requirements included in the Organization's HITRUST assessment mapped to the NY OHIP requirement averaged 66 - 89.99%.
FC	Fully Compliant: The control maturity level's scores across all HITRUST CSF requirements included in the Organization's HITRUST assessment mapped to the NY OHIP requirement averaged 90 - 100%.

AC - Access Controls

AC - Reference	Requirement	Implemented Scoring
AC-1	Policy and Procedures	FC
AC-2	Account Management	FC
AC-2(1)	Automated System Account Management	FC
AC-2(3)	Disable Accounts	FC
AC-2(4)	Automated Audit Actions	FC
AC-2(5)	Inactivity Logout	FC
AC-2(7)	Privileged User Accounts	FC
AC-2(9)	Restrictions on Use of Shared and Groups Accounts	FC
AC-2(12)	Account Monitoring for Atypical Usage	FC
AC-2(13)	Disable Accounts For High-Risk Individuals	FC
AC-3	Access Enforcement	FC
AC-3(9)	Controlled Release	FC
AC-3(14)	Individual Access	FC
AC-4	Information Flow Environment	FC
AC-5	Separation of Duties	FC
AC-6	Least Privilege	FC
AC-6(1)	Authorize Access to Security Functions	FC
AC-6(2)	Non-Privileged Access for Non-Security Functions	FC
AC-6(3)	Network Access to Privileged Commands	FC
AC-6(5)	Privileged Accounts	FC
AC-6(7)	Review of User Privileges	FC
AC-6(9)	Auditing Use of Privileged Functions	FC
AC-6(10)	Prohibit Non-Privileged Users From Executing Privileged Functions	FC
AC-7	Unsuccessful Logon Attempts	FC

AC - Reference	Requirement	Implemented Scoring
AC-7(2)	Purge or Wipe Mobile Devices	FC
AC-8	System Use Notification	FC
AC-9	Previous Logon Notification	FC
AC-9(1)	Unsuccessful Logons	FC
AC-11	Device Lock	FC
AC-11(1)	Pattern-Hiding Displays	FC
AC-12	Session Termination	FC
AC-14	Permitted Actions Without Identification or Authentication	FC
AC-17	Remote Access	FC
AC-17(1)	Automated Monitoring / Control	FC
AC-17(2)	Protection of Confidentiality and Integrity Using Encryption	FC
AC-17(3)	Managed Access Control Points	FC
AC-17(4)	Privileged Commands and Access	FC
AC-18	Wireless Access	FC
AC-18(1)	Authentication and Encryption	FC
AC-18(3)	Disable Wireless Networking	FC
AC-18(4)	Wireless Access | Restrict Configurations by Users	FC
AC-18(5)	Wireless Access | Antennas and Transmission Power Levels	FC
AC-19	Access Control for Mobile Devices	FC
AC-19(5)	Full Device and Container-based Encryption	FC
AC-20	Use of External Information Systems	FC
AC-20(1)	Limits on Authorized Use	FC
AC-20(2)	Portable Storage Devices — Restricted Use	FC
AC-20(3)	Non-organizationally Owned Systems — Restricted Use	FC
AC-21	Information Sharing	FC

AC - Reference	Requirement	Implemented Scoring
AC-22	Publicly Accessible Content	FC

AT - Awareness Training

AT - Reference	Requirement	Implemented Scoring
AT-1	Policy and Procedures	FC
AT-2	Literacy Training and Awareness	FC
AT-2(2)	Insider Threat	FC
AT-2(3)	Social Engineering and Mining	FC
AT-3	Role-Based Training	FC
AT-3(5)	Processing Personally Identifiable Information	FC
AT-4	Training Records	FC

This section has been truncated for the sample report

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 customers.
Application(s)	Penguin Nest, Penguin Analytics, South Pole Benefits Eligibility
Database Type(s)	Oracle
Operating System(s)	HP-UX

Customer Central (a.k.a. "Portal")	
Residing Facility	CP Framingham Manufacturing Facility
Exclusion(s) from scope	Content and applications from customer systems that are delivered via the Portal are outside the scope of this assessment. This includes customers who choose to leverage the embedded credit card processing page, which is offered as an add-on service. The embedded credit processing page is provided and managed by a third-party service provider.

In-Scope Facilities

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

Facility Name	Type of Facility	Third-party Managed?	Third-party Provider	City	State	Country
Pelican Data Center	Data Center	Yes	Pelican Hosting	Salt Lake City	UT	United States of America
CP Headquarters	Office	No	-	Salt Lake City	UT	United States of America
CP Framingham Manufacturing Facility	Office	No	-	Framingham	MA	United States of America

Services Outsourced

The following table presents outsourced services relevant to the scope of this assessment. The "Consideration in this Assessment" column of this table specifies the method utilized for each service provider relevant to the scope of this e1 assessment. Organizations undergoing e1 assessments have two options of how to address situations in which a HITRUST CSF requirement is fully or partially performed by a service provider (e.g., by a cloud service provider):

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

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

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

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).

Limitations of Assurance

- This Insights Report provides transparency into the current state of NY OHIP coverage and control maturity within the scoped environment for the Organization as described in the 'Coverage and Reportability' section above. This Insights Report supports the Organization in communicating the status of controls supporting NY OHIP Compliance and is not a certification of NY OHIP Compliance.
    - This Insights 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 NY OHIP compliance across the entirety of the Organization. Parties relying on this report should therefore evaluate the Scope in relation to the Organization's NY OHIP obligations in consultation with 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 NY OHIP compliance and were not designed to specifically detect all instances of NY OHIP non-compliance.
    - Compliance deficiencies noted in this report, if any, were identified through an evaluation of control maturity of the HITRUST CSF requirements mapping to NY OHIP included in the Organization's HITRUST validated assessment and not in observance of any other criteria specific to NY OHIP requirements.
- Mappings produced by HITRUST to authoritative sources are performed utilizing the NIST OLIR Program methodology outlined in NIST Interagency Report 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.

NY OHIP Overview

The New York State Office of Health Insurance Programs (OHIP) is responsible for providing guidance and oversight for Medicaid related information systems, programs and business processes at the Department of Health (DOH). This responsibility includes defining business, information, and technical guidance that will create a common security framework for IT system implementations responsible for protecting DOH Medicaid data. OHIP extends this guidance to entities with whom DOH provided Medicaid data is shared.

OHIP has defined the Moderate-Plus Security Controls Baseline based on, and consistent with, the security provisions described in the Centers for Medicare and Medicaid Services (CMS) Acceptable Risk Safeguards (ARS) and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 at the Moderate level with enhancements that are necessary to comply with New York State (NYS) Policies and Standards. The additional NYS controls represent the “Plus” in the OHIP Moderate-Plus Security Controls Baseline.

The OHIP Moderate-Plus Security Controls Baseline is organized according to the 20 security control families as set forth in CMS ARS and NIST SP 800-53:

- Access Control (AC)
- Awareness and Training (AT)
- Audit and Accountability (AU)
- Security Assessment and Authorization (CA)
- Configuration Management (CM)
- Contingency Planning (CP)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental Protection (PE)
- Planning (PL)
- Program Management (PM)
- Personnel Security (PS)
- PII Processing and Transparency (PT)
- Risk Assessment (RA)
- System and Services Acquisition (SA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)
- Supply Chain Risk Management (SR)

NY OHIP Coverage and Reportability

A HITRUST validated assessment can provide evidence that specific HITRUST CSF control requirements mapping to NY OHIP Moderate-Plus Security Controls Baseline have been implemented, how well they have been implemented, and the nature and volume of identified gaps in implementation. The HITRUST CSF, the inherent mappings to NY OHIP Moderate-Plus Security Controls Baseline as a supported authoritative source, and HITRUST's comprehensive assurance program are important tools for organizations with Moderate-Plus Security Controls Baseline compliance obligations.

The following factors collectively determine the degree of Moderate-Plus Security Controls Baseline coverage and reportability in a HITRUST assessment:

- HITRUST's approach to incorporating Moderate-Plus Security Controls Baseline into the HITRUST CSF
- The Organization's assessment type selection and HITRUST CSF version selection

Approach to incorporating NY OHIP into the HITRUST CSF:

The HIRUST CSF maps to the NY OHIP Moderate-Plus Security Controls Baseline by mapping to the control descriptions and implementation standards of the System Security Plan (SSP) workbook for each of the 20 control families outlined in the previous section. For certain controls, the implementation standards are categorized into different levels (low, moderate, and/or high). For those implementation standards, HITRUST maps only to the moderate level.

Appendix A: NY OHIP - Relevant Observations

During the HITRUST assessment accompanying this NY OHIP Insights Report, the implemented control maturity level on each of the following HITRUST CSF requirements scored less than "Fully Compliant". These conditions were identified as relevant to the Organization's NY OHIP compliance efforts, as each of these HITRUST CSF requirements map to one or more NY OHIP requirements. The relying party should evaluate these items (and the associated risk treatment) in consultation with the Organization.

IA - Identification and Authentication

Reference	Mapped HITRUST CSF Requirement	Maturity level(s) scoring less than fully compliant	Management's stated corrective actions (unvalidated)
IA-1a1b, IA-1b, IA-1[IS.1a1b], IA-1[IS.1b]	Mapped BUID: 01.00aNIST80053Organizational.29 / CVID: 2578.0. The organization develops, documents, and disseminates to designated organization-defined personnel or roles an organization-level identification and authentication policy that is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines, and designates an organization-defined official to manage the development, documentation, and dissemination of the identification and authentication policy and procedures.	Implemented	No corrective action plans were communicated to HITRUST for this condition.

MA - Maintenance

Reference	Mapped HITRUST CSF Requirement	Maturity level(s) scoring less than fully compliant	Management's stated corrective actions (unvalidated)
MA-1a1b, MA-1b, MA-1[IS.1a1b], MA-1[IS.1b]	Mapped BUID: 01.00aNIST80053Organizational.42 / CVID: 2658.0. The organization develops, documents, and disseminates to designated organization-defined personnel or roles an organization-level system maintenance policy that is	Implemented	No corrective action plans were communicated to HITRUST for this condition.

Reference	Mapped HITRUST CSF Requirement	Maturity level(s) scoring less than fully compliant	Management's stated corrective actions (unvalidated)
	consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines, and designates an organization-defined official to manage the development, documentation, and dissemination of the organization-level system maintenance policy and procedures.		

MP - Media Protection

Reference	Mapped HITRUST CSF Requirement	Maturity level(s) scoring less than fully compliant	Management's stated corrective actions (unvalidated)
MP-4b, MP-4[IS.2]	Mapped BUID: 18127.08l1Organizational.3 / CVID: 0812.0. The organization ensures that surplus equipment is stored securely while not in use, and disposed of or sanitized when no longer required.	Implemented	No corrective action plans were communicated to HITRUST for this condition.

Appendix B: Relevant HITRUST Assessment Results and Mappings

Below are the assessment results and control maturity evaluations for each assessed HITRUST CSF requirement mapped to the areas of NY OHIP considered in the underlying HITRUST CSF assessment, organized by NY OHIP control family.

In addition to this authoritative Source, the HITRUST CSF is mapped to dozens of additional authoritative sources, 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.

AC - Access Controls

HITRUST CSF Requirement	Implemented Score
AC-1 - Policy and Procedures	
AC-1a1a - (a) Develop, document, and disseminate to applicable personnel and roles: 1. An access control policy that: a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	
Mapped BUID: 11.01aFedRAMPOrganizational.1 / CVID: 2494.0. The organization develops, documents, and disseminates to organization-defined personnel or roles an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the access control policy and associated access controls. The organization reviews and updates the current access control policy at least annually and access control procedures at least annually or whenever a significant change occurs.	Fully Compliant

HITRUST CSF Requirement	Implemented Score
AC-1a1b - (a) Develop, document, and disseminate to applicable personnel and roles: 1. An access control policy that: b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and	
Mapped BUID: 01.01aNIST80053Organizational.2 / CVID: 2580.0. The organization develops, documents, and disseminates to designated organization-defined personnel or roles an organization-level access control policy that is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines, and designates an organization-defined official to manage the development, documentation, and dissemination of the access control policy and procedures.	Fully Compliant

AC-1a2 - (a) Develop, document, and disseminate to applicable personnel and roles: 2. Procedures that are defined within the applicable control implementation statements of the associated AC controls.	
Mapped BUID: 11.01aFedRAMPOrganizational.1 / CVID: 2494.0. The organization develops, documents, and disseminates to organization-defined personnel or roles an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the access control policy and associated access controls. The organization reviews and updates the current access control policy at least annually and access control procedures at least annually or whenever a significant change occurs.	Fully Compliant

AC-1b - (b) Designate defined officials (e.g., Senior Management such as the CISO, SOP), Mission/Business-defined officials and System-defined officials (e.g., Business Owner, System Owner, ISSO) to manage the development, documentation, and dissemination of the access control policy and procedures; and	
Mapped BUID: 01.01aNIST80053Organizational.2 / CVID: 2580.0. The organization develops, documents, and disseminates to designated organization-defined personnel or roles an organization-level access control policy that is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines, and designates an organization-defined official to manage the development, documentation, and dissemination of the access control policy and procedures.	Fully Compliant

HITRUST CSF Requirement	Implemented Score
AC-1c1 - (c) Review and update the current access control: 1. Policy at least every one (1) years and following CMS-defined events (e.g., assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).; and	
Mapped BUID: 11.01aFedRAMPOrganizational.1 / CVID: 2494.0. The organization develops, documents, and disseminates to organization-defined personnel or roles an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the access control policy and associated access controls. The organization reviews and updates the current access control policy at least annually and access control procedures at least annually or whenever a significant change occurs.	Fully Compliant
AC-1c2 - (c) Review and update the current access control: 2. Procedures at least every one (1) years and following CMS-defined events (e.g., assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).	
Mapped BUID: 11.01aFedRAMPOrganizational.1 / CVID: 2494.0. The organization develops, documents, and disseminates to organization-defined personnel or roles an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the access control policy and associated access controls. The organization reviews and updates the current access control policy at least annually and access control procedures at least annually or whenever a significant change occurs.	Fully Compliant
AC-1[PHI.1] - Systems processing, storing, or transmitting PII (to include PHI): PHI.1 - Develop, disseminate, and review/update the access control policies and procedures that comply with the HIPAA Minimum Necessary Rule, which includes permitted or required uses and disclosures, to limit unnecessary or inappropriate access to PHI.	
Mapped BUID: 11.01aFedRAMPOrganizational.1 / CVID: 2494.0. The organization develops, documents, and disseminates to organization-defined personnel or roles an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the access control policy and associated access controls. The organization reviews and	Fully Compliant

HITRUST CSF Requirement	Implemented Score
updates the current access control policy at least annually and access control procedures at least annually or whenever a significant change occurs.	
Mapped BUID: 01.01aNIST80053Organizational.2 / CVID: 2580.0. The organization develops, documents, and disseminates to designated organization-defined personnel or roles an organization-level access control policy that is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines, and designates an organization-defined official to manage the development, documentation, and dissemination of the access control policy and procedures.	Fully Compliant

AC-1[PHI.2] - Systems processing, storing, or transmitting PII (to include PHI): PHI.2 - Policies and procedures to comply with the regulatory requirements governing an individual's right to access copies of their PHI, including electronic copies.	
Mapped BUID: 01.01aNIST80053Organizational.2 / CVID: 2580.0. The organization develops, documents, and disseminates to designated organization-defined personnel or roles an organization-level access control policy that is consistent with applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines, and designates an organization-defined official to manage the development, documentation, and dissemination of the access control policy and procedures.	Fully Compliant

AC-2 - Account Management

AC-2a - (a) Define and document the type of accounts allowed and specifically prohibited for use within the system (e.g., individual, group, system, application, guest/anonymous, emergency, and temporary);	
Mapped BUID: 1139.01b2System.10 / CVID: 0023.0. The organization ensures account types are identified (individual, shared/group, system, application, guest/anonymous, emergency, and temporary) and conditions for group and role membership are established. If used, shared/group account credentials are modified when users are removed from the group.	Fully Compliant

This section has been truncated for the 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.