HITRUST

NIST SP 800-171 Insights

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

Chinstrap Penguin Corp

As of October 1, 2026

View this assessment in the **HITRUST Report Center**

HITRUST

Contents

Transmittal Letter

October 1, 2026

Chinstrap Penguin Corp
123 Main Street
Anytown, Texas 12345

Through HITRUST's "Assess Once, Report Many" capability made possible through the HITRUST CSF, HITRUST has prepared this NIST SP 800-171 Revision 3: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations ("NIST SP 800-171") 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 NIST SP 800-171 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 NIST SP 800-171 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 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

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.

Section 3 of NIST SP 800-171 requires organizations to conduct a risk assessment, specifically to 'assess the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI' and to 'update risk assessments' at an organization-defined frequency. 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 3.11.01 of NIST SP 800-171.

Management of the Organization is also solely responsible for ensuring the Organization's compliance with any legal and/or regulatory requirements, including NIST SP 800-171.

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 NIST SP 800-171, 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.

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

HITRUST

NIST SP 800-171 Scorecard

The tables below provide insights on NIST SP 800-171 compliance for the environment assessed. Each NIST SP 800-171 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 NIST SP 800-171 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

MC	Mostly Compliant: The control maturity level's scores across all HITRUST CSF requirements included in the Organization's HITRUST assessment mapped to the NIST SP 800-171 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 NIST SP 800-171 requirement averaged 90 - 100%.
Not Applicable	Not Applicable: All HITRUST CSF requirements included in the Organization's HITRUST assessment mapped to the NIST SP 800-171 requirement were deemed not applicable by the Organization. The Organization's N/A rationale can be found in Appendix B of this document.
Not Evaluated	Not Evaluated: No HITRUST CSF requirements were included in the Organization's HITRUST assessment which mapped to the NIST SP 800-171 requirement.

HITRUST

Access Control

Reference	Requirement	Implemented Scoring
03.01.01: Account Management		
03.01.01.a	Account Management	Not Evaluated
03.01.01.b	Account Management	Not Evaluated
03.01.01.c.01	Account Management	MC
03.01.01.c.02	Account Management	FC
03.01.01.c.03	Account Management	MC
03.01.01.d.01	Account Management	MC
03.01.01.d.02	Account Management	MC
03.01.01.e	Account Management	FC
03.01.01.f.01	Account Management	FC
03.01.01.f.02	Account Management	FC
03.01.01.f.03	Account Management	FC
03.01.01.f.04	Account Management	FC
03.01.01.f.05	Account Management	FC
03.01.01.g.01	Account Management	FC
03.01.01.g.02	Account Management	FC
03.01.01.g.03	Account Management	FC
03.01.01.h	Account Management	FC

This section has been truncated for this sample report

HITRUST

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	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 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

HITRUST

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).

Assessment Utilized	Assessed Entity	Assessment Type	Utilization Approach	Relevant Platforms	Relevant Facilities	Assessment Domains
Pelican Hosting HITRUST r2	Pelican Hosting	HITRUST r2	Inheritance	(All in-scope platforms)	(All in-scope facilities)	(All assessment domains)

HITRUST

Limitations of Assurance

- This Insights Report provides transparency into the current state of NIST 800-171 r3 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 NIST 800-171 r3 Compliance and is not a certification of NIST 800-171 r3 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 NIST 800-171 r3 compliance across the entirety of the Organization. Parties relying on this report should therefore evaluate the Scope in relation to the Organization's NIST 800-171 r3 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 NIST 800-171 r3 compliance and were not designed to specifically detect all instances of NIST 800-171 r3 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 NIST 800-171 r3 included in the Organization's HITRUST validated assessment and not in observance of any other criteria specific to NIST 800-171 r3 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.

HITRUST

NIST SP 800-171 Overview

Controlled Unclassified Information (CUI) is information that is not classified but requires a level of protection from unauthorized access and release. Executive Order 13556 established the CUI Program to standardize practices for handling CUI across federal and nonfederal agencies and departments. Through CUI regulations, federal agencies using federal systems to process, store, or transmit CUI are required to comply with NIST standards and guidelines. When federal agencies share CUI with nonfederal organizations, their responsibility for protecting the information does not change.

NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations contains the recommended security requirements for protecting the confidentiality of CUI when it is processed, stored, or transmitted by nonfederal organizations and systems. The security requirements in NIST SP 800-171 are derived from the controls in NIST SP 800-53 and are recommended to be incorporated into contracts and agreements between federal agencies and nonfederal organizations when CUI is involved.

The list below outlines the sections of NIST SP 800-171:

- Section 1: Sets out the purposes of NIST SP 800-171, explains the parties that NIST SP 800-171 applies to, and describes the organization of the publication.
- Section 2: Describes the assumptions and methodology used to develop the security requirements for protecting the confidentiality of CUI, the format of the requirements, and the tailoring criteria applied to the NIST guidelines to obtain the requirements.
- Section 3: Lists the security requirements for protecting the confidentiality of CUI in nonfederal systems and organizations.

These security requirements are organized in the following security requirement families:

- Access Control
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment
- Security Assessment and Monitoring
- System and Communications Protection
- System and Information Integrity
- Planning

- System and Services Acquisition
- Supply Chain Risk Management

The remaining sections, References, Appendix A: Acronyms, Appendix B: Glossary, Appendix C: Tailoring Criteria, Appendix D: Organization-Defined Parameters, and Appendix E: Change Log provide additional information to support the guidelines.

NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information, is an additional publication which outlines the assessment procedures and methodology for assessing the security requirements defined in NIST SP 800-171.

The list below outlines the sections of NIST SP 800-171A:

- Section 1: sets out the purposes of NIST SP 800-171A, explains the parties that NIST SP 800-171A applies to, and describes the organization of the publication.
- Section 2: explains the structure and content of the procedures provided in Section 3.
- Section 3: provides the assessment procedures for the security requirements defined in NIST SP 800-171. The assessment procedures are organized in the same 17 security requirement families used to organize the security requirements in NIST SP 800-171.

The remaining sections, References, Appendix A: Acronyms, Appendix B: Glossary, Appendix C: Security Requirement Assessments, Appendix D: Organization-Defined Parameters, and Appendix E: Change Log provide additional information to support the guidelines.

HITRUST

NIST SP 800-171 Coverage and Reportability

A HITRUST validated assessment provides evidence that specific HITRUST CSF control requirements mapping to Section 3, The Security Requirements of NIST SP 800-171, 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 NIST SP 800-171 as a supported authoritative source, and HITRUST's comprehensive assurance program are important tools for organizations with NIST SP 800-171 compliance obligations.

The following factors collectively determine the degree of NIST SP 800-171 coverage and reportability in a HITRUST assessment:

- HITRUST's approach to incorporating NIST SP 800-171 into the HITRUST CSF
- The Organization's assessment type selection, HITRUST CSF version selection, and assessment tailoring

Approach to incorporating NIST SP 800-171 into the HITRUST CSF:

NIST 171-800A provides determination statements (beginning with “Determine if”) which offer instruction for assessing each security requirement discussed in NIST SP 800-171. HITRUST has harmonized NIST SP 800-171 and NIST SP 800-171A into the HITRUST CSF by establishing cross-references (i.e., maps) between HITRUST CSF requirement statements and applicable NIST SP 800-171A determination statements. In addition to the determination statements, NIST SP 800-171A includes organizational-defined parameters (ODP) where necessary. See below an example of how the determination statements and ODPs in NIST 800-171A align with the security requirements in NIST 800-171.

NIST 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	NIST 800-171A Assessing Security Requirements for Controlled Unclassified Information
03.01.06 Least Privilege – Privileged Accounts a. Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles]. b. Require that users (or roles) with privileged accounts use non-privileged accounts when accessing non-security functions or non-security information.	Determine if: A.03.01.06.ODP[01]: personnel or roles to which privileged accounts on the system are to be restricted are defined. A.03.01.06.a: privileged accounts on the system are restricted to A.03.01.06.ODP[01]: personnel or roles. A.03.01.06.b: users (or roles) with privileged accounts are required to use non-privileged accounts when accessing non-security functions or non-security information.

By mapping to all determination statements in Section 3 of NIST 800-171A, the HITRUST CSF effectively maps to all security requirements in Section 3 of NIST 800-171.

The HITRUST CSF intentionally does not provide full coverage of NIST SP 800-171 and intentionally does not contain mappings or cross-references to all text in NIST SP 800-171.

Like many other authoritative sources, NIST SP 800-171 contains several sections that are not directly actionable by organizations needing to achieve or evaluate compliance. The non-actionable sections are concentrated at the beginning (Section 1. Introduction and Section 2. The Fundamentals) and ending (References, Appendix A: Acronyms, Appendix B: Glossary, Appendix C: Tailoring Criteria, Appendix D: Organization-Defined Parameters, and Appendix E: Change Log).

The HITRUST CSF's coverage of NIST SP 800-171 at a high level, is as follows:

Impact of assessment preferences and tailoring on NIST 800-171 coverage and reportability

HITRUST assessments are performed against a subset of HITRUST CSF's numerous requirements. The requirements included in the accompanying HITRUST Risk-based, 2-year (r2) assessment have been tailored based on the unique risks and compliance needs of the Organization and on the HITRUST CSF version selected by the Organization (v11.4.0).

Through tailoring, organizations can optionally add authoritative sources into their r2 assessments. When this occurs, the assessment is expanded to consider additional requirements mapping to the information security and/or privacy-related portions of the included authoritative sources. The resulting, tailored HITRUST r2 assessment then serves to directly evaluate the Organization's adherence to a subset of the HITRUST CSF and indirectly evaluate the assessed entity's compliance with the information security and/or privacy aspects of the included authoritative source(s).

The HITRUST CSF is constantly updated by HITRUST in response to changes in the cybersecurity threat landscape and updates to included authoritative sources. Organizations can utilize the most recent HITRUST CSF version in HITRUST r2 assessments or can optionally utilize one of many prior HITRUST CSF versions. As HITRUST advances the framework, more and better reporting capabilities are unlocked. Not all versions allow for the HITRUST insights reporting against all portions of NIST SP 800-171; instead, only assessments utilizing version 11.4 and later can create NIST SP 800-171 Insights Reports.

HITRUST

Appendix A: NIST SP 800-171-relevant Observations

During the HITRUST assessment accompanying this NIST SP 800-171 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 NIST SP 800-171 compliance efforts, as each of these HITRUST CSF requirements map to one or more NIST SP 800-171 requirements. The relying party should evaluate these items (and the associated risk treatment) in consultation with the Organization.

Reference	Mapped HITRUST CSF Requirement	Maturity level(s) scoring less than fully compliant	Management's stated corrective actions (unvalidated)
03.01.01.c.01, 03.01.01.c.03, 03.01.01.d.01, 03.01.01.d.02, 03.01.05.a	**Mapped BUID: 1143.01c1System.123 / CVID: 0035.0.** The allocation of privileges for all systems and system components is controlled through a formal authorization process. The organization ensures access privileges associated with each system product (e.g., operating system, database management system and each application) and the users associated with each system product which need to be allocated are identified. Privileges are allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy (e.g., the minimum requirement for their functional role–user or administrator, only when needed).	Implemented	No corrective action plans were communicated to HITRUST for this condition.

HITRUST

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 NIST SP 800-171 considered in the underlying HITRUST CSF assessment, organized by NIST SP 800-171 part.

This section also shows the HITRUST CSF requirements mapped by HITRUST to each considered NIST SP 800-171 requirement. Note that many more mappings exist between NIST SP 800-171 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 NIST SP 800-171 Coverage and Reportability section of this document.

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.

Note that one or more NIST SP 800-171 requirements were intentionally omitted from this section due to their inapplicability to the Organization and/or lack of coverage in the underlying HITRUST CSF assessment—these NIST SP 800-171 requirements are, however, shown in the "NIST SP 800-171 Scorecard" section of this document.

HITRUST

3.1 - Access Control

HITRUST CSF Requirement	Implemented Score
03.01.01 - Account Management	
03.01.01.c.01 - Specify: Authorized users of the system	
Mapped BUID: 1143.01c1System.123 / CVID: 0035.0. The allocation of privileges for all systems and system components is controlled through a formal authorization process. The organization ensures access privileges associated with each system product (e.g., operating system, database management system and each application) and the users associated with each system product which need to be allocated are identified. Privileges are allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy (e.g., the minimum requirement for their functional role–user or administrator, only when needed).	Mostly Compliant
03.01.01.c.02 - Specify: Group and role membership	
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
03.01.01.c.03 - Specify: Access authorizations (i.e., privileges) for each account	
Mapped BUID: 1143.01c1System.123 / CVID: 0035.0. The allocation of privileges for all systems and system components is controlled through a formal authorization process. The organization ensures access privileges associated with each system product (e.g., operating system, database management system and each application) and the users associated with each system product which need to be allocated are identified. Privileges are allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy	Mostly Compliant

HITRUST CSF Requirement	Implemented Score
(e.g., the minimum requirement for their functional role–user or administrator, only when needed).	

03.01.01.d.01 - Authorize access to the system based on: A valid access authorization	
Mapped BUID: 1143.01c1System.123 / CVID: 0035.0. The allocation of privileges for all systems and system components is controlled through a formal authorization process. The organization ensures access privileges associated with each system product (e.g., operating system, database management system and each application) and the users associated with each system product which need to be allocated are identified. Privileges are allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy (e.g., the minimum requirement for their functional role–user or administrator, only when needed).	Mostly Compliant

This section has been truncated for this sample report

HITRUST

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.