GovRAMP Insights

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

Chinstrap Penguin Corp

As of October 1, 2025

SAMPLE REPORT FOR ILLUSTRATIVE USE ONLY

View this assessment in the HITRUST Report Center

Contents

Transmittal Letter

October 1, 2025

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 GovRAMP ("GovRAMP") 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 the NIST SP 800-53 r5 overlay for GovRAMP impact level moderate for the scope outlined below, based on control validation procedures executed during a HITRUST Essentials, 1-year (e1) validated assessment using v11.6.0 of the HITRUST CSF. The Organization can leverage this report to share information regarding their GovRAMP compliance efforts with internal and external stakeholders.

The full e1 validated report contains detailed information relating to the maturity of information protection controls as defined by the scoping 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 Essentials, 1-year (e1) validated assessment.

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

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 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.

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

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

HITRUST's Responsibilities

HITRUST is responsible for maintenance of the HITRUST CSF and HITRUST Assurance Program against which the Organization completed the accompanying Essentials, 1-year (e1) validated assessment. HITRUST is also responsible for producing the mappings from various authoritative sources, including GovRAMP, 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

HITRUST

GovRAMP Scorecard

The tables below provide GovRAMP implementation statuses for each control (e.g., AC-1) and sub-control (e.g., AC-1a1a) in the NIST SP 800-53 r5 overlay for GovRAMP impact level moderate for the environment assessed. A subset of controls within NIST 800-53 r5 must be fully implemented—without exception—in order to achieve GovRAMP authorization. The tables below also indicate which NIST 800-53 r5 controls are “minimum mandatory controls” in the GovRAMP overlay for impact level moderate. Control observations associated with NIST 800-53 controls, if present, are discussed in Appendix A.

These GovRAMP implementation statuses are based on the HITRUST assessment results of the mapped HITRUST CSF requirement(s). Where more than one HITRUST CSF requirement mapped to a control or sub-control, a low-watermark approach is used to derive the GovRAMP implementation status. For example, a NIST SP 800-53 control with two mapped HITRUST CSF requirements—one with a control maturity of less than "Fully Compliant" in the HITRUST implemented control maturity and the other without—would result in a GovRAMP implementation status of “Planned”. Note that GovRAMP's "Alternative Implementation" status is excluded from this scorecard given that it cannot be reached through performance of a HITRUST CSF assessment.

Note that the Organization may have in place additional controls that support compliance with the NIST SP 800-53 overlay for GovRAMP impact level moderate which were not evaluated in the underlying HITRUST assessment and therefore not reflected in this scoring.

The tables below also show the HITRUST assessment results for the HITRUST implemented control maturity level. 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 GovRAMP 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 GovRAMP 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 GovRAMP requirement averaged 90 - 100%.
Not Applicable	Not Applicable: All HITRUST CSF requirements included in the Organization's HITRUST assessment mapped to the GovRAMP 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 GovRAMP requirement.

GovRAMP Implementation Status Legend

Planned	The control / sub-control was not yet implemented by the Organization, but there was a plan and a timeline to implement it in the future. For example, an Organization may have a planned status for a control that requires a new software update or a configuration change that is scheduled for a later date. The planned status is documented in the system security plan (SSP) and the plan of action and milestones (POA&M) of the Organization.
Partially Implemented	The Organization had implemented some, but not all, of the sub-controls (e.g., AC-2b) within this control (e.g., AC-2).
Implemented	The control / sub-control was fully implemented by the Organization.
Not Applicable	The control / sub-control was deemed not relevant to the system or the system environment by the Organization. For example, a control that requires physical security measures may not be applicable to a cloud service that does not have physical access to the data center. In this case, the Organization would document the not applicable status in the control implementation summary (CIS) worksheet and explain why the control is not applicable to the system.

GovRAMP performs a review of assessment procedures and results prior to issuing GovRAMP authorization. The GovRAMP implementation statuses shown in this Insights Report have not been reviewed by GovRAMP and could be subject to change as a result of GovRAMP’s review; they should therefore be viewed as preliminary.

MODERATE ACCESS CONTROL - MODERATE ACCESS CONTROL

NIST SP 800-53 Control	GovRAMP Minimum-Mandated Control?	GovRAMP Implementation Status (Pending GovRAMP's review)	Count of NIST SP 800-53 Sub-Controls with Implemented Observation(s)
AC-17(2)[M] . Remote Access - Protection of Confidentiality and Integrity Using Encryption	Yes	Implemented	0
AC-17[M] . Remote Access	Yes	Implemented	0
AC-2(1)[M] . Account Management - Automated System Account Management	Yes	Implemented	0
AC-2(7)[M] . Account Management - Privileged User Accounts	Yes	Implemented	0
AC-2[M] . Account Management	Yes	Planned	4
AC-4[M] . Information Flow Enforcement	Yes	Implemented	0
AC-6(10)[M] . Least Privilege - Prohibit Non-privileged Users from Executing Privileged Functions	Yes	Implemented	0
AC-6(2)[M] . Least Privilege - Non-privileged Access for Nonsecurity Functions	Yes	Implemented	0
AC-6[M] . Least Privilege	Yes	Not Applicable	
AC-1[M] . Policy and Procedures	No	Implemented	0
AC-11(1)[M] . Device Lock - Pattern-hiding Displays	No	Implemented	0
AC-11[M] . Device Lock	No	Implemented	0
AC-12[M] . Session Termination	No	Implemented	0
AC-14[M] . Permitted Actions Without Identification or Authentication	No	Implemented	0
AC-17(1)[M] . Remote Access - Monitoring and Control	No	Implemented	0
AC-17(3)[M] . Remote Access - Managed Access Control Points	No	Implemented	0
AC-17(4)[M] . Remote Access - Privileged Commands and Access	No	Implemented	0

This section has been truncated for this sample report

GovRAMP Overview

In 2020, a Steering Committee comprised of dozens of current and former State Chief Information Officers, Chief Information Security Officers, Procurement and Privacy Officials joined private industry leaders and cyber assessing organizations to charter GovRAMP.

GovRAMP brings state and local governments together to develop standards for cloud security, educate on best practices, and recognize a common method for verifying the cloud security of service providers who use or offer cloud solutions that process, store, and/or transmit government required data, including personally identifiable information (PII), personal health information (PHI) and payment card industry (PCI) information.

GovRAMP launched in 2021 and is organized as a 501c6 non-profit organization, governed by a majority of state and local government officials, with minority representation from private industry and subject matter experts.

Like FedRAMP, GovRAMP's process for verification relies on FedRAMP Authorized Third Party Assessing Organizations (3PAOs) to conduct independent audits and assessments. The requirements are built on the widely accepted National Institute of Standards and Technology (NIST) Special Publication 800- 53 Rev. 4 framework, soon to be Rev. 5.

With GovRAMP, Procurement Officials, Privacy Officers, and Information Security Officers can be confident in knowing government-selected service providers meet and maintain published cybersecurity policies.

Secure service providers have the ability to grow their government business at scale through transferrable cybersecurity verifications published on GovRAMP's Approved Vendor List.

GovRAMP formalizes processes that allow third party assessment organizations to validate IaaS, SaaS, and PaaS solutions to ensure service providers meet government-published cybersecurity policies.

GovRAMP Coverage and Reportability

A HITRUST validated assessment provides evidence that specific HITRUST CSF control requirements that map to the NIST SP 800-53 r5 overlay for GovRAMP impact level moderate have been implemented, measures how well they have been implemented, and documents the nature and volume of any identified gaps in implementation. The HITRUST CSF, the inherent mapping to NIST SP 800-53 r5 overlay for GovRAMP impact level moderate as a supported authoritative source, and the robust and comprehensive security assurance program are important tools for those seeking to obtain or maintain authorization from GovRAMP. The following factors collectively determine the degree of GovRAMP coverage in a HITRUST assessment:

- The Organization's assessment preferences and tailoring
- The Organization's GovRAMP impact level (e.g., moderate)

Assessment preferences and tailoring

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 to the unique risks and compliance needs of the Organization.

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. Further, NIST periodically releases updated revisions to SP 800-53. When this occurs, GovRAMP updates its overlays of NIST SP 800-53.

Organizations seeking HITRUST CSF r2 certification 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 the GovRAMP overlay of NIST SP 800-53. Insights Reports support for each GovRAMP overlay of NIST SP 800-53, by CSF version, is as follows:

- GovRAMP low and moderate impact overlays of NIST SP 800-53 r5: CSF version 11.3.0 and later

The HITRUST assessment underlying this GovRAMP Insights Report utilized HITRUST CSF version 11.3.0.

GovRAMP Impact Level

GovRAMP Security Controls are defined in three categories of impact levels, with each impact level featuring its own GovRAMP-defined overlay of NIST SP 800-53:

- Low: Aligned with Low Impact, based on FedRAMP Low Control Baselines

- Moderate: Aligned with Moderate Impact, based on FedRAMP Moderate Control Baselines

- High: GovRAMP recognizes FedRAMP High Control Baselines

NIST SP 800-53 r5 impact level overlay selected by the Organization	Impact level: Moderate

Assessment Context

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

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

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

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

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

Use of the Work of Others

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

Inheritance of assessment results from another, previously completed HITRUST validated assessment is the only option available for using the work of others allowed by both HITRUST and GovRAMP. HITRUST also allows for reliance on third-party assurance reports (e.g., SOC2 Type 2 reports) in lieu of direct testing when certain requirements are met; however, this approach is not supported by GovRAMP and cannot be leveraged in a HITRUST CSF assessment being submitted to GovRAMP for authorization consideration.

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)

Limitations of Assurance

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

- This Insights Report provides transparency into the current state of GovRAMP 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 GovRAMP compliance and is not a certification of GovRAMP compliance.

- This Insights Report accompanies a HITRUST CSF e1 Validated assessment. The accompanying e1 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:

  - 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 GovRAMP compliance and were not designed to specifically detect all instances of GovRAMP 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 GovRAMP included in the Organization's HITRUST validated assessment and not in observance of any other criteria specific to GovRAMP 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.

Appendix A: GovRAMP-relevant Observations

During the HITRUST Risk-based, 2-year (r2) Validated Assessment accompanying this GovRAMP 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 GovRAMP authorization efforts, as each of these HITRUST CSF requirements map to one or more controls within the NIST SP 800-53 r5 overlay for GovRAMP impact level moderate. Note that one or more of these observations may lack a stated corrective action plan (CAP); this is due to the fact that only a subset of these observations may have required a CAP per HITRUST's Assurance Program Requirements. These items and their associated risk treatment should be evaluated in consultation with the Organization.

A subset of controls within NIST 800-53 r5 must be fully implemented—without exception—in order to achieve GovRAMP authorization. If any were noted during the HITRUST CSF validated assessment, observations associated with these “minimum mandatory controls” are listed separately in this appendix.

Refer to Section A.1 (Observations Within Minimum Mandatory Controls) and Section A.2 (Other Observations) below

Appendix A.1: Observations Related To Minimum Necessary Controls

MODERATE ACCESS CONTROL

Reference	Mapped HITRUST CSF Requirement	Maturity level(s) scoring less than fully compliant	Management's stated corrective actions (unvalidated)
AC-2e[M], AC-2i1[M], AC-2i2[M], AC-2i3[M]	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	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)
	(e.g., the minimum requirement for their functional role–user or administrator, only when needed).		

Appendix A.2: Other Observations

MODERATE CONFIGURATION MANAGEMENT

Reference	Mapped HITRUST CSF Requirement	Maturity level(s) scoring less than fully compliant	Management's stated corrective actions (unvalidated)
CM-12b[M]	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.

This section has been truncated for this sample report

Appendix B: Relevant HITRUST Assessment Results and Mappings

Below are the HITRUST assessment results and control maturity evaluations for each assessed HITRUST CSF requirement mapped to the areas of the NIST SP 800-53 r5 overlay for GovRAMP impact level moderate. 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.

In addition to the NIST SP 800-53 r5 overlay for GovRAMP impact level moderate, 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 are not reviewed by or endorsed by external regulatory bodies, and instead undergo at least five levels of internal HITRUST review before being finalized: automated review, initial mapper review, peer review, management review, and quality assurance review. Questions or concerns about these mappings should be routed to HITRUST's Support team.

Note that one or more GovRAMP 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 GovRAMP requirements are, however, shown in the "GovRAMP Scorecard" section of this document.

MODERATE ACCESS CONTROL

NIST 800-53 Control Requirement	AC-17(2)[M]: Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
Additional GovRAMP Parameters and Guidance	None
Mapped HITRUST CSF Requirement Statement	BUID: 0903.10f1Organizational.1 / CVID: 1289.0. Encryption is used to protect covered and/or confidential information transported by mobile or removable media and across communication lines. Encryption procedures supporting the encryption policy address the required level of protection (e.g., the type and strength of the encryption algorithm required), and specifications for the effective implementation throughout the organization (e.g., which solution is used for which business processes).
Implemented Score	Fully Compliant (100%)
Inherited?	No
Assessed Entity Commentary	None

External Assessor Commentary	None
Assessment Evidence	None

NIST 800-53 Control Requirement	AC-17a[M]: a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
Additional GovRAMP Parameters and Guidance	None
Mapped HITRUST CSF Requirement Statement	BUID: 11.01nFedRAMPOrganizational.2 / CVID: 2375.0. The organization establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed. Remote access to the information system is authorized prior to allowing such connections.
Implemented Score	Fully Compliant (100%)
Inherited?	No
Assessed Entity Commentary	None
External Assessor Commentary	None
Assessment Evidence	None

This section has been truncated for this sample report

Appendix C: HITRUST Background

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

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

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

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

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

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

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