HITRUST

Health Industry Cybersecurity Practices (HICP) v2023 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 Health Industry Cybersecurity Practices (HICP) v2023 (“HICP”) Insights Report at the request of Chinstrap Penguin Corporation ('the Organization'). This Insights Report contains detailed information relating to the coverage and maturity of controls supporting the Organization's compliance with aspects of HICP for the scope outlined below, based on control validation procedures executed during a HITRUST Risk-based, 2-year (r2) Validated Assessment using v11.4.0 of the HITRUST CSF. The Organization can leverage this report to share information regarding their HICP compliance efforts with internal and external stakeholders.

The full r2 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.

Cybersecurity Practice #10: Cybersecurity Oversight and Governance of HICP 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 Cybersecurity Practice #10: Cybersecurity Oversight and Governance of HICP.

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

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

HICP Scorecard

The tables below provide insights on HICP compliance for the environment assessed. Each HICP requirement listed is assigned a compliance score for the policy, procedure, and implemented control maturity levels. The compliance scores are based on the assessment results of the HITRUST CSF requirement(s) as mapped to the HICP 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.

The Organization may have in place additional controls relevant to their HICP compliance posture which were not evaluated in the underlying HITRUST assessment and therefore not reflected in this report.

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

FC	Fully Compliant: The control maturity level's scores across all HITRUST CSF requirements included in the Organization's HITRUST assessment mapped to the HICP requirement averaged 90 - 100%.
Not Applicable	Not Applicable: All HITRUST CSF requirements included in the Organization's HITRUST assessment mapped to the HICP requirement were deemed not applicable by the Organization. The Organization's N/A rationale can be found in Appendix B of this document.

HITRUST

Email Protection Systems

Email Protection Systems - Reference	Requirement	Implemented Scoring
1: Cybersecurity Practice #1: Email Protection Systems		
1.L.A	Advanced and Next-Generation Tooling	FC
1.L.B	Digital Signatures	FC
1.L.C	Analytics-Driven Education	FC
1.M.A	Basic Email Protection Controls	FC
1.M.B	Multi-Factor Authentication for Email Access	FC
1.M.C	Email Encryption	FC
1.M.D	Workforce Education	FC
1.S.A	Email System Configuration	FC
1.S.B	Education	FC
1.S.C	Phishing Simulations	FC

Endpoint Protection Systems

Endpoint Protection Systems - Reference	Requirement	Implemented Scoring
2: Cybersecurity Practice #2: Endpoint Protection Systems		
2.L.A	Automate the Provisioning of Endpoints	FC
2.L.B	Host-Based Intrusion Detection and Prevention Systems	FC
2.L.C	Endpoint Detection and Response	FC
2.L.D	Application Allowlisting	FC
2.L.E	Micro-Segmentation/Virtualization Strategies	FC
2.M.A	Basic Endpoint Protection Controls	FC
2.M.B	Mobile Device and Mobile Application Management	Not Applicable
2.S.A	Basic Endpoint Protection Controls	FC

This section has been truncated for this sample report

HITRUST

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).

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 procedures performed by the external assessor, including those where the external assessor utilized the work of others, were subject to HITRUST's quality assurance review procedures. The table below details assessments utilized by the external assessor.

Potential options available for using the work of others allowed by HITRUST's Assurance Program Requirements include the following and are reflected in the "Utilization Approach" column of the below table if leveraged in this assessment:

- Inheritance of results from or reliance on another HITRUST validated assessment,
- Reliance on a recent third-party assurance report, and/or
- Reliance on testing performed by the assessed entity (i.e., by internal assessors).

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

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 Health Industry Cybersecurity Practices (HICP) coverage and control maturity within the scoped environment for the Organization as described in the 'Coverage and Reportability' section herein. This Insights Report supports the Organization in communicating the status of controls supporting HICP compliance and is not a certification of HICP 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 HICP compliance across the entirety of the Organization. Parties relying on this report should therefore evaluate the Scope in relation to the Organization's HICP 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 HICP compliance and were not designed to specifically detect all instances of HICP 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 HICP included in the Organization's HITRUST validated assessment and not in observance of any other criteria specific to HICP 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

HICP Overview

The Health Industry Cybersecurity Practices (HICP) is a framework developed by the US Department of Health and Human Services (HHS) that contains a set of guidelines, best practices, and recommendations to help healthcare organizations of all sizes strengthen their cybersecurity practices.

HICP has three stated goals:

- Cost-effectively reduce cybersecurity risks for the Healthcare and Public Health (HPH) sector
- Support the voluntary adoption and implementation of its recommendations; and
- Ensure that content is actionable, practical and relevant to healthcare stakeholders of every size and resource level on an ongoing basis.

The HICP publication defines ten common cybersecurity practices (CSPs):

- CSP 1. Email Protection Systems
- CSP 2. Endpoint Protection Systems
- CSP 3. Access Management
- CSP 4. Data Protection and Loss Prevention
- CSP 5. Asset Management
- CSP 6. Network Management
- CSP 7. Vulnerability Management
- CSP 8. Security Operation Centers and Incident Response
- CSP 9. Network Connected Medical Devices
- CSP 10. Cybersecurity Oversight and Governance

For each of the ten CSPs, HICP outlines sub-practices that are tailored to small, medium, and large organizations. :

The list below outlines the sections of HICP:

- The Main Document discusses the purpose of the HICP publication and describes the cybersecurity threats currently faced by healthcare organization.
- Technical Volume 1 outlines the sub-practices specific to small healthcare organizations.
- Technical Volume 2 outlines the sub-practices specific to medium and to large healthcare organizations.
- The Resources and Templates document provide additional resources and references.

HITRUST

HICP Coverage and Reportability

A HITRUST validated assessment provides evidence that specific HITRUST CSF control requirements mapping to the ten cybersecurity practices of HICP 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 HICP as a supported authoritative source, and HITRUST's comprehensive assurance program are important tools for organizations with HICP compliance obligations.

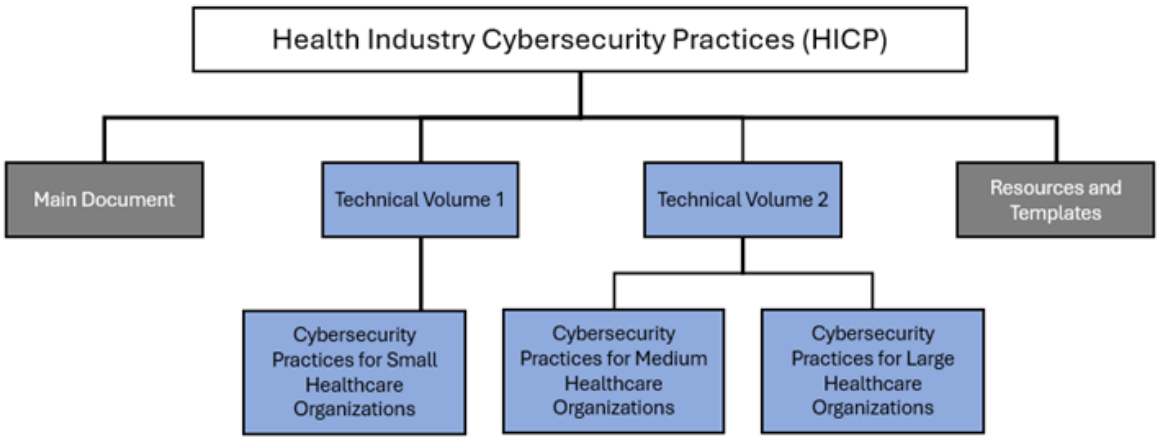
The following factors collectively determine the degree of HICP coverage and reportability in a HITRUST assessment:

- HITRUST's approach to incorporating HICP into the HITRUST CSF
- The Organization's assessment type selection, HITRUST CSF version selection, and assessment tailoring
- The Organization’s size (small, medium, and/or large), as asserted by the Organization in accordance with guidance outlined in Table 1 of HICP’s Main Document. This table’s guidance helps organizations consider attributes such as number of physicians, beds, dedicated IT professionals, and health information exchange partners when making this determination.

Approach to incorporating HICP into the HITRUST CSF.

The HIRUST CSF maps to the HICP cybersecurity sub-practices for small, medium, and large organizations. These sub-practices are found in the Technical Volume 1 and Technical Volume 2 documents of the HICP publication.

The HITRUST CSF’s coverage of HICP at a high level, is as follows:



Within the Cybersecurity Practices for Medium Healthcare Organizations, there is one sub-practice, 9.M.F, that was intentionally not mapped to the HITRUST CSF. The 9.M.F sub-practice contains an assignment of rights which is not actionable to organizations seeking to evaluate compliance with HICP.

9.M.F: If an HDO discovers (or is notified) of a high-risk cybersecurity vulnerability and cannot receive support from the medical device manufacturer to mitigate this risk, the HDO has recourse to contact the FDA directly to file a complaint concern about the vulnerability. FDA contact should be limited to critical or high-risk scenarios, especially those with the potential to cause harm to patients.

Impact of assessment preferences and tailoring on HICP 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 HICP; instead, only assessments utilizing version 11.3 and later can create HICP Insights Reports.

Organizational characteristics impacting HICP applicability and coverage

The HICP publication acknowledges that the process of implementing cybersecurity controls varies based on an organizations size and complexity. HICP therefore presents separate sets of cybersecurity sub-practices for small, medium, and large organizations.

Specific to the HITRUST assessment scope, characteristics affecting the applicability of HICP requirements considered in the HITRUST r2 assessment underlying this HICP Insights Report are as follows:

Small, Medium, and/or Large	Small

HITRUST

Appendix A: HICP-Relevant Observations

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

HITRUST CSF Requirement	Maturity level(s) scoring less than fully compliant	Management's stated corrective actions (unvalidated)
3.M.B - Provisioning, Transfers and Deprovisioning Procedures: Provisioning, Transfers and Deprovisioning Procedures		
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

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 HICP considered in the underlying HITRUST CSF assessment, organized by HICP part.

This section also shows the HITRUST CSF requirements mapped by HITRUST to each considered HICP requirement. Note that many more mappings exist between HICP 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 HICP 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 HICP 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 HICP requirements are, however, shown in the "HICP Scorecard" section of this document.

HITRUST CSF Requirement	Implemented Score
1 - Cybersecurity Practice #1: Email Protection Systems	
1.L.C - Analytics-Driven Education	
Mapped BUID: 069.06g2Organizational.56 / CVID: 0604.0. The internal security organization regularly reviews the compliance of information processing as part of a formal risk assessment process. The security organization maintains records of the compliance results (e.g., organization-defined metrics) in order to better track security trends within the organization, respond to the results of correlation and analysis, and to address longer term areas of concern.	Fully Compliant

HITRUST

HITRUST CSF Requirement	Implemented Score
1.M.A - Basic Email Protection Controls	
Mapped BUID: 0207.09j1Organizational.6 / CVID: 0880.0. Centrally managed spam protection mechanisms are employed at information system entry and exit points, workstations, servers, and mobile computing devices on the network. Spam protection mechanisms detect and take action on unsolicited messages transported by electronic mail, transported by electronic mail attachments, transported by Web accesses, transported by other common means, and inserted through the exploitation of information system vulnerabilities. Malicious code and spam protection mechanisms are centrally managed and updated when new releases are made available in accordance with the organization's configuration management policy and procedures.	Fully Compliant
Mapped BUID: 13100.02eNYDOHOrganizational.4 / CVID: 2073.0. Information security and privacy education and awareness training must address individuals' responsibilities associated with sending sensitive information in email.	Fully Compliant
Mapped BUID: 0931.09v1Organizational.8 / CVID: 0886.1. The organization has implemented Sender Policy Framework (SPF) by deploying SPF records in DNS, enabled receiver-side verification in mail servers to lower the chance of spoofed email messages, implemented DomainKeys Identified Mail (DKIM) to allow receiving servers to verify that email messages actually came from the organization, and implemented Domain-based Message Authentication, Reporting and Conformance (DMARC) to tell receiving servers to either quarantine or reject emails from the organization that don't pass SPF or DKIM.	Fully 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.