HITRUST

Health Industry Cybersecurity Practices (HICP) v2023 Insights

Based upon a HITRUST Risk-based, 2-year (r2) Validated Assessment

Chinstrap Penguin Corporation

As of February 26, 2024

SAMPLE FOR ILLUSTRATIVE USE ONLY

HITRUST

Contents

1. Transmittal Letter

February 26, 2024

Chinstrap Penguin Corporation
123 Main Street
Anytown, TX 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 Corp. ("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 r2 assessment that this Insights Report is based upon included the following of the Organization ("Scope"):

Platform:

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

Facility:

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

HITRUST

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 Risk-based, 2-year (r2) Validated Assessment, the Organization asserted that management of the Organization:

- Is responsible for the implementation of information protection controls.
- Has made available to the HITRUST External Assessor all records and necessary documentation related to the information protection controls included within the scope of the Risk-based, 2-year (r2) Validated Assessment.
- 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 Risk-based, 2-year (r2) 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 Risk-based, 2-year (r2) Validated 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 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 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 HICP, 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

2. 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) mapped to the HICP requirement. These mappings can be found in Appendix B of this document. 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

SC	Somewhat 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 11 - 32.99%.
MC	Mostly Compliant: The control maturity level's scores across all HITRUST CSF requirements included in the Organization's HITRUST assessment mapped to the HICP 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 HICP requirement averaged 90 - 100%.
Does Not Apply	Does Not Apply: Based on information provided by the Organization (as outlined in the "Scope of the Assessment" and "Organizational characteristics impacting HICP " sections of this document), the HICP requirement does not apply to the scoped aspects of the Organization.

HITRUST

1 - Email Protection Systems

Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
1.L. Sub-Practices for Large-Sized Organizations				
1.L.A	Advanced and Next-Generation Tooling	MC	FC	MC
1.L.B	Digital Signatures	FC	FC	FC
1.L.C	Analytics-Driven Education	FC	FC	FC
1.M. Sub-Practices for Medium-Sized Organizations				
1.M.A	Basic Email Protection Controls	FC	FC	FC
1.M.B	Multi-Factor Authentication for Email Access	FC	FC	FC
1.M.C	Email Encryption	FC	FC	FC
1.M.D	Workforce Education	FC	FC	FC
1.S. Sub-Practices for Small Organizations				
1.S.A	Email System Configuration	FC	FC	FC
1.S.B	Education	FC	FC	FC
1.S.C	Phishing Simulations	FC	FC	FC

2 - Endpoint Protection Systems

Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
2.L. Sub-Practices for Large-Sized Organizations				
2.L.A	Automate the Provisioning of Endpoints	FC	FC	FC
2.L.B	Host-Based Intrusion Detection and Prevention Systems	FC	FC	FC
2.L.C	Endpoint Detection and Response	FC	FC	FC
2.L.D	Application Allowlisting	FC	FC	FC
2.L.E	Micro-Segmentation/Virtualization Strategies	FC	FC	MC
2.M. Sub-Practices for Medium-Sized Organizations				
2.M.A	Basic Endpoint Protection Controls	FC	FC	FC
2.M.B	Mobile Device and Mobile Application Management	FC	FC	FC
2.S. Sub-Practices for Small Organizations				
2.S.A	Basic Endpoint Protection Controls	FC	FC	FC

This table has been truncated for this sample report

HITRUST

3. Assessment Context

About the HITRUST r2 Assessment and Certification

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

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

Assessment Approach

An *Authorized HITRUST External Assessor Organization* (the "External Assessor") performed validation procedures to measure the control maturity of the HITRUST CSF requirements and corresponding evaluative elements included in this assessment for the scope of the assessment. These validation procedures were designed by the External Assessor based upon the assessment's scope in observance of HITRUST's CSF Assurance Program Requirements and consisted of inquiry with key personnel, inspection of evidence (e.g. access lists, logs, configuration, sample items, policies, procedures, diagrams), on-site or virtual observations, (optionally) utilization of the work of others (as described elsewhere in this report), and (optionally) reperformance of controls.

Each requirement in the HITRUST CSF contains one or more evaluative elements. For example, requirement 0322.09u2Organizational.12, which reads "Media is encrypted when onsite unless physical security can be guaranteed, and always when offsite.", contains the following two evaluative elements: "1. The organization restricts the use of writable, removable media in organizational systems" and "2. The organization restricts the use of personally owned, removable media in organizational systems". The implementation and operation of all evaluative elements associated with applicable HITRUST CSF requirements included in the assessment was evaluated by the External Assessor in reaching an implementation score.

Implementation Score	Description	Points Awarded
Not compliant-(NC)	Very few if any of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment. Rough numeric equivalent of 0% (point estimate) or 0% to 10% (interval estimate).	0

Implementation Score	Description	Points Awarded
Somewhat complaint (SC)	Some of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 25% (point estimate) or 11% to 32% (interval estimate).	25
Partially compliant (PC)	About half of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 50% (point estimate) or 33% to 65% (interval estimate).	50
Mostly compliant (MC)	Many but not all of the evaluative elements in HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 75% (point estimate) or 66% to 89% (interval estimate).	75
Fully compliant (FC)	Most if not all of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 100% (point estimate) or 90% to 100% (interval estimate).	100

Risk Factors

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

Assessment Type	
HITRUST Risk-based, 2-year (r2) Security Assessment	
General Risk Factors	
Do you offer Infrastructure as a Service (IaaS)?	No
Organization Type	Service Provider (Information Technology, IT)
Organizational Risk Factors	
Number of Records that are currently held	Between 10 and 60 Million Records
Technical Risk Factors	

Does the organization allow personally owned devices to connect to scoped organizational assets (i.e., BYOD - bring your own device)?	Yes
Is any aspect of the scoped environment hosted on the cloud?	No - testing
Is scoped information sent by the organization using courier services, internal mail services, or external mail services (e.g., USPS)?	Yes
Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component?	No - testing
Does the scoped environment allow dial-up/dial-in capabilities (i.e., functional analog modems)?	No - testing
Does the organization allow the use of electronic signatures to provide legally binding consent within the scoped environment, e.g., simple or basic electronic signatures (SES), advanced electronic or digital signature (AES), or qualified advanced electronic or digital signatures (QES)?	No - testing
Does the system allow users to access the scoped environment from an external network that is not controlled by the organization?	Yes
Is scoped information sent and/or received via fax machine (i.e., an actual machine, excluding efax or scan to email)?	No - testing
Does the organization use any part of the scoped systems, system components, or system services to sell goods and/or services?	Yes
Is the system(s) accessible from the Internet?	Yes
Number of interfaces to other systems	25 to 75
Number of transactions per day	6,750 to 85,000
Number of users of the system(s)	Fewer than 500
Is the system(s) publicly positioned?	No - testing
Is the scoped system(s) (on-premises or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)?	No - testing
Does the system(s) transmit or receive data with a third-party?	No - testing
Are hardware tokens used as an authentication method within the scoped environment?	No - testing
Do any of the organization's personnel travel to locations the organization deems to be of significant risk?	No - testing

Are wireless access points in place at any of the organization's in-scope facilities?	No - testing

Compliance Factors (Optional)
HICP 2023 Edition > For Large Orgs.
HICP 2023 Edition > For Medium Orgs.
HICP 2023 Edition > For Small Orgs.
Ontario Personal Health Information Protection Act > Health Data Institute
StateRAMP r5 > Impact level: Moderate
AI Risk Management > NIST AI RMF & ISO/IEC 23894
NIST SP 800-171 r3

4. 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 Platforms

The following tables 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

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

In-Scope Facilities

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

Facility Name	Type of Facility	Third-party Managed	Third-party provider	City	State	Country
CP Framingham Manufacturing Facility	Other	No	(None)	Framingham	Massachusetts	United States of America
CP Headquarters and Manufacturing	Office	No	(None)	Las Vegas	Nevada	United States of America
Pelican Data Center	Data Center	Yes	Pelican Hosting	Salt Lake City	Utah	United States of America

Services Outsourced

The following table presents outsourced services relevant to the scope of this assessment. The "Consideration in this Assessment" column of this table specifies the method utilized for each service provider relevant to the scope of this r2 assessment. HITRUST requires the inclusive method must be used on HITRUST r2 validated assessments. Under the Inclusive method, HITRUST CSF requirements performed by the

service provider are included within the scope of the assessment and addressed through full or partial inheritance, reliance on third-party assurance reports, and/or direct testing by the external assessor.

Third-party Provider	Relevant Service(s) Provided	Consideration in this Assessment
Seashore Offsite Data Storage	Seashore provides backup tape delivery and storage in a secure offsite facility. No customer, covered, otherwise confidential information is stored at Seashore's facilities, however.	Included
Pelican Hosting	Pelican Hosting provides a colocation facility where Chinstrap Penguin maintains a dedicated cage. Pelican Hosting personnel do not have logical access to any in-scope systems.	Included

5. Use of the Work of Others

An Authorized HITRUST External Assessor Organization (i.e., the external assessor) performed procedures to validate the Organization's asserted control maturity scores. These validation procedures were designed by the external assessor based upon the assessment's scope in observance of HITRUST's Assurance Program Requirements and consisted of inquiry with key personnel, inspection of system-generated evidence (e.g., access lists, logs, configurations, sample items), on-site or virtual observations, and (optionally) reperformance of controls.

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 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 Organization (i.e., by internal assessors).

Assessment Utilized	Assessed Entity	Assessment Type	Report Date(s)	Utilization Approach	Relevant Platforms	Relevant Facilities	Assessment Domains
Pelican Hosting HITRUST r2	Pelican Hosting	HITRUST r2	2/29/22	Inheritance	(All in-scope platforms)	(All in-scope facilities)	(All assessment domains)

HITRUST

6. 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 HICP 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 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 management systems, physical facilities, and IT platforms. Therefore, the HITRUST assessment may be scoped differently than an assessment focused exclusively to 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

7. 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:

1. Cost-effectively reduce cybersecurity risks for the Healthcare and Public Health (HPH) sector;

2. Support the voluntary adoption and implementation of its recommendations; and

3. 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):

ID	Title
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.

8. HICP Coverage and Reportability

A HITRUST validated assessment can provide 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.

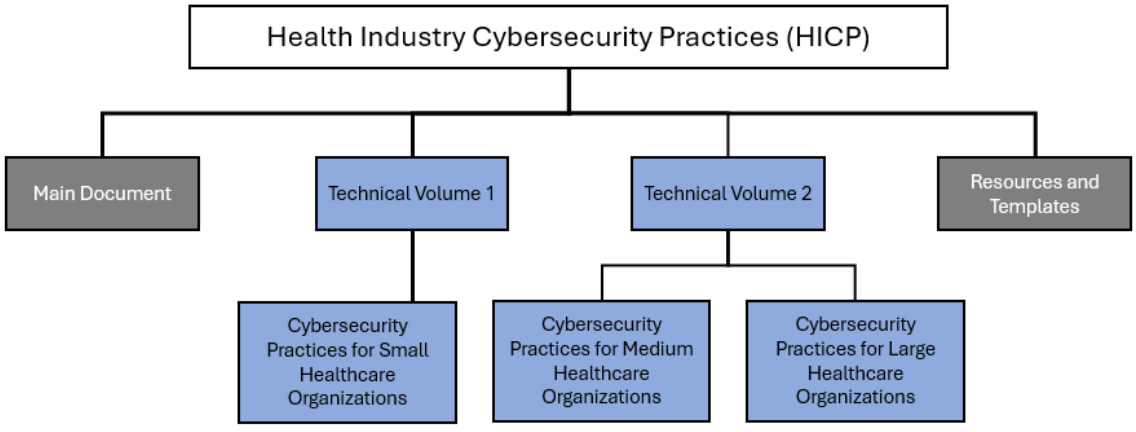
The following factors collectively determine the degree of HICP coverage and reportability in a HITRUST assessment:

- 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 self-selected "size" (small, medium, or large) per HICP's organization size definition guidance

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:



Color	Meaning
Grey	Not mapped to the HITRUST CSF because not security related
Blue	Mapped to the HITRUST CSF

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 HITRUST 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 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 11.4.0 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:

Organization Size per HICP Guidance:	Large, Medium, Small

HITRUST

Appendix A: HICP-relevant Observations

During the HITRUST assessment accompanying this HICP Insights Report, the policy, process, and/or 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.

1 - Email Protection Systems

Reference	Mapped HITRUST CSF Requirement	Maturity level(s) scoring less than fully compliant	Management's stated corrective actions (unvalidated)
1.L.A	**BUID: 02.09jHICPOrganizational.4 / CVID: 2334.0** . The organization uses an advanced protection technology to automatically remove email messages from the inbox of all users if a message is determined to be malicious after delivery.	Policy	No corrective action plans were communicated to HITRUST for this condition.

Appendix A 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

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 HICP, 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.

1 - Email Protection Systems

HITRUST CSF Requirement	Policy Score	Procedure Score	Implemented Score
Cybersecurity Practice #1: Email Protection Systems			
1.S.A. Email System Configuration			
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	Fully Compliant	Mostly Compliant	Somewhat Compliant

HITRUST CSF Requirement	Policy Score	Procedure Score	Implemented Score
made available in accordance with the organization's configuration management policy and procedures.			
BUID: 0226.09k1Organizational.2 / CVID: 0896.0 . The organization implements and regularly updates mobile code protection, including anti-virus and anti-spyware.	Fully Compliant	Mostly Compliant	Somewhat Compliant
BUID: 0627.10h1System.45 / CVID: 1303.0 . Vendor supplied software used in operational systems is maintained at a level supported by the supplier and uses the latest version of Web browsers on operational systems to take advantage of the latest security functions. The organization maintains information systems according to a current baseline configuration and configures system security parameters to prevent misuse.	Fully Compliant	Mostly Compliant	Somewhat Compliant
BUID: 09.09v1Organizational.7 / CVID: 2365.0 . The organization uses an email filtering solution to recognize and block suspicious emails and unnecessary file types before they reach employee inboxes.	Fully Compliant	Mostly Compliant	Somewhat Compliant
BUID: 11113.01q3System.3 / CVID: 0215.0 . The organization employs multifactor authentication for remote network access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access. The organization employs multifactor authentication for local access to privileged accounts (including those used for non-local maintenance and diagnostic sessions).	Fully Compliant	Mostly Compliant	Somewhat Compliant
BUID: 17.10aHICPOrganizational.2 / CVID: 2324.0 . The organization does not use free or consumer e-mail systems for business purposes.	Fully Compliant	Mostly Compliant	Somewhat Compliant
BUID: 1784.10aHICPOrganizational.2 / CVID: 1230.0 . Where the security functionality in a proposed product does not satisfy the specified requirement, then the risk introduced and associated controls are reconsidered prior to purchasing the product.	Fully Compliant	Mostly Compliant	Somewhat Compliant
BUID: 19134.06dNYDOHOrganizational.9 / CVID: 0035.0 . The information system protects the confidentiality and integrity of personally identifiable information (PII).	Fully Compliant	Mostly Compliant	Somewhat Compliant

Cybersecurity Practice #2: Endpoint Protection Systems

HITRUST CSF Requirement	Policy Score	Procedure Score	Implemented Score
BUID: 0226.09k1Organizational.2 / CVID: 0896.0 . The organization implements and regularly updates mobile code protection, including anti-virus and anti-spyware.	Fully Compliant	Mostly Compliant	Somewhat Compliant
BUID: 0221.09jFTIOrganizational.1 / CVID: 0891.0 . The organization establishes policies governing the installation of software by users, enforces software installation policies through automated methods, and monitors software installation policy compliance on a continual basis.	Fully Compliant	Mostly Compliant	Somewhat Compliant
BUID: 0265.09m1Organizational.2 / CVID: 0943.2 . The organization applies a default-deny rule that drops all traffic via host-based firewalls or port filtering tools on its endpoints (workstations, servers, etc.), except those services and ports that are explicitly allowed.	Fully Compliant	Mostly Compliant	Somewhat Compliant

Appendix B 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 a harmonized information protection framework that incorporates and leverages the existing security requirements placed upon organizations, including international (e.g., GDPR, ISO), federal (e.g., FFIEC, HIPAA), state / province (e.g., PHIPA, CCPA), third party (e.g., PCI, COBIT), and other government agencies (e.g., NIST, FTC, 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.