HITRUST

Ransomware Insights

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

Chinstrap Penguin Corp.

As of December 3, 2025

SAMPLE REPORT FOR ILLUSTRATIVE USE ONLY

View this assessment in the
HITRUST Report Center

HITRUST

Contents

HITRUST
6175 Main Street
Suite 400
Frisco, TX 75034

View this assessment in the HITRUST Report Center

Transmittal Letter

December 3, 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 thisRansomware Threat Insights Report at the request of Chinstrap Penguin Corp. ("the Organization"). For the scope outlined below, this Insights Report contains detailed information relating the Organization's ability to counter ransomware threats and deal with the potential consequences of events. The Organization can leverage this report to share information regarding the posture of controls relevant to the threat of ransomware with internal and external stakeholders.

This report's findings are based on control validation procedures executed during a HITRUSTEssentials, 1-year (e1) validated assessment using v11.7.0 of the HITRUST CSF. The full e1 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.

Information in this Insights Report is presented using the NIST Cybersecurity Framework (CSF) version 2.0 by incorporating guidance outlined in a NIST CSF v2.0 Community Profile focusing on ransomware risk management: NIST Internal Report (IR) 8374 revision 1. This NIST Internal Report identifies the security objectives from the NIST CSF 2.0 that support governing management of, identifying, protecting against, detecting, responding to, and recovering from ransomware events.

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

- Pelican Data Center (Data Center) 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, including Ransomware.

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 Ransomware, 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

Ransomware Scorecard

This Ransomware Scorecard shows the control maturity of the Organization's NIST CSF v2.0 subcategories relevant to managing the risk of ransomware events. The purpose of this scorecard is to help the Organization gauge and/or communicate its level of readiness to counter ransomware threats and to deal with the potential consequences of ransomware events. It can also be used to identify opportunities for improving cybersecurity to help thwart ransomware. It prioritizes security objectives from the NIST CSF 2.0 that help to govern management of, identify, protect against, detect, respond to, and recover from ransomware events.

This scorecard brings the following two inputs together:

- The NIST CSF 2.0 Ransomware Community Profile discussed in NIST IR 8374 revision 1, which was developed by NIST in collaboration with industry to serve as a baseline of NIST CSF outcomes prioritized for relevance to ransomware risk management.

- Results of control validation (testing) procedures executed by the Organization's External Assessor during a HITRUST Essentials, 1-year (e1) validated assessment using v11.7.0 of the HITRUST CSF.

The control maturity levels shown are the aggregated scores for the underlying HITRUST CSF requirements as they are mapped by HITRUST to the subset of NIST Cybersecurity Framework core functions, categories, and subcategories prioritized in the Ransomware Community Profile as being particularly relevant to mitigating ransomware risk (priority 1 items especially so).

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 Ransomware requirement averaged 90 - 100%.

HITRUST

GOVERN

GOVERN (GV): The organizations cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored

NIST CSF Core Item	Priority	Ransomware Application	Implemented Scoring	Observations noted in this asmt.
GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	2	Organizational mission helps establish risk-based ransomware approach and prioritize based on critical services.	FC	0
GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	2	Stakeholder needs can help inform ransomware risk decisions, including ransom payment and communication strategies.	FC	0
GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity including privacy and civil liberties obligations are understood and managed	2	Legal, regulatory, and contractual requirements regarding cybersecurity are understood and managed. For example, some laws set specific reporting requirements; organizations should understand their reporting obligations prior to an incident. Further, organizations should understand when paying a ransom is permitted or prohibited by law.	FC	0

HITRUST

NIST CSF Core Item	Priority	Ransomware Application	Implemented Scoring	Observations noted in this asmt.
GV.OC-04: Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated	2	Understanding the critical services that internal and external stakeholders depend on can inform the prioritization of ransomware defenses and recovery processes.	FC	0
GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated	2	Understanding dependencies, including those on other organizations or services, is important in preparing for ransomware events, as critical services may be rendered inoperable if dependent services are impacted by ransomware.	FC	0

This section has been truncated for this sample report

HITRUST

Assessment Context

About the HITRUST e1 Assessment and Certification

HITRUST e1 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 an 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 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).

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.

HITRUST

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.

HITRUST developed a scoring rubric that is used by External Assessors to determine implementation scoring in a consistent and repeatable way by evaluating both implementation strength and implementation coverage, described as follows:

- The HITRUST CSF requirement's implementation strength is evaluated using a 5-point scale (tier 0 through tier 4) by considering the requirement's implementation and operation across the assessment scope, which consists of all organizational and system elements, including the physical facilities and logical systems / platforms, within the defined scope of the assessment.

- The HITRUST CSF requirement's implementation coverage is evaluated using a 5-point scale (very low through very high) by considering the percentage of the requirement's evaluative elements implemented and operating within the scope of the assessment.

The implementation scoring model utilized on e1 assessments incorporates the following scale. The overall score for each HITRUST CSF requirement ranges from 0 to 100 points in quarter increments based directly on the requirement's 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
Somewhat Compliant (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

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

Customer Central (a.k.a. "Portal")	
	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
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	Office	No	-	Framingham	MA	United States of America
Pelican Data Center	Data Center	Yes	-	Salt Lake City	UT	United States of America

HITRUST

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, the external assessor may have utilized the work of other assessors, auditors, and/or inspectors in lieu of direct testing. All assessment Use of the Work of Others, including those where the external assessor utilized the work of others, were subject to HITRUST's quality assurance review procedures. The table below details assessments utilized by the external assessor.

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

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

Work of other assessors was not relied upon in the HITRUST CSF assessment underlying this compliance insights report (i.e., no inheritance or third-party reliance was utilized).

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 coverage and maturity of controls supporting the organization's ability to prevent and respond to the threat of ransomware within the scoped environment for the Organization. This Insights Report supports the Organization in communicating the status of such controls and is not a certification.

- This Insights Report accompanies a HITRUST 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:

    - 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 the Organization’s ability to prevent, detect, and correct ransomware attacks across the entirety of the Organization. Parties relying on this report should therefore evaluate the Scope.

    - 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 the Organization's ability to prevent, detect, and correct ransomware attacks.

    - Control deficiencies noted in this report, if any, were identified through an evaluation of control maturity of the HITRUST CSF requirements related to preventing, detecting, and correcting ransomware included in the Organization's HITRUST validated assessment and not in observance of any other criteria specific to ransomware.

- No assessment of controls or compliance status provides total assurance or 100% protection against possible control failures threats.

HITRUST

Ransomware Overview

Ransomware continues to be one of the most formidable cybersecurity challenges facing organizations worldwide. This malicious software encrypts critical data, rendering systems inoperable until a ransom is paid, often in cryptocurrency. The threat has evolved beyond mere encryption; modern ransomware attacks frequently involve data exfiltration and attackers threats to publish or sell stolen data as well.

In 2024, ransomware incidents reached unprecedented levels. Rapid7 reported over 2,570 publicly disclosed ransomware attacks in the first half of the year alone, averaging 14 incidents per day. The total number of attacks for the year was estimated at 5,414, marking an 11% increase from 2023.

Ransomware operators have become more sophisticated, employing tactics such as:

- Double Extortion: Encrypting data and threatening to release sensitive information publicly if the ransom is not paid.
- Triple Extortion: Adding Distributed Denial of Service (DDoS) attacks to pressure victims further.
- Ransomware-as-a-Service (RaaS): Offering ransomware tools to affiliates, lowering the barrier to entry for cybercriminals and expanding the threat landscape.

These tactics have increased the complexity and impact of ransomware attacks, making them more challenging to prevent and mitigate.

The consequences of ransomware attacks are severe and far-reaching:

- Financial Losses: The FBI reported that ransomware cost U.S. victims $16.6 billion in 2024, a 33% increase from the previous year.
- Operational Disruption: Attacks have crippled critical infrastructure, including healthcare, education, and government services.
- Reputational Damage: Data breaches resulting from ransomware can erode customer trust and damage an organization's reputation.

HITRUST

Ransomware remains a dynamic and escalating threat in 2025. While improved defenses and law enforcement efforts have led to a decrease in ransom payments, the frequency and sophistication of attacks continue to rise. Organizations must remain vigilant, adopting proactive and layered security measures to protect against this persistent menace.

HITRUST

The NIST CSF and Ransomware Community Profile

The NIST Cybersecurity Framework

The NIST Cybersecurity Framework complements rather than replaces an organization's existing risk management process and cybersecurity program by providing an overarching set of guidelines to provide a minimal level of consistency as well as depth, breadth, and rigor of industry's cybersecurity programs, as shown in Figure 1.

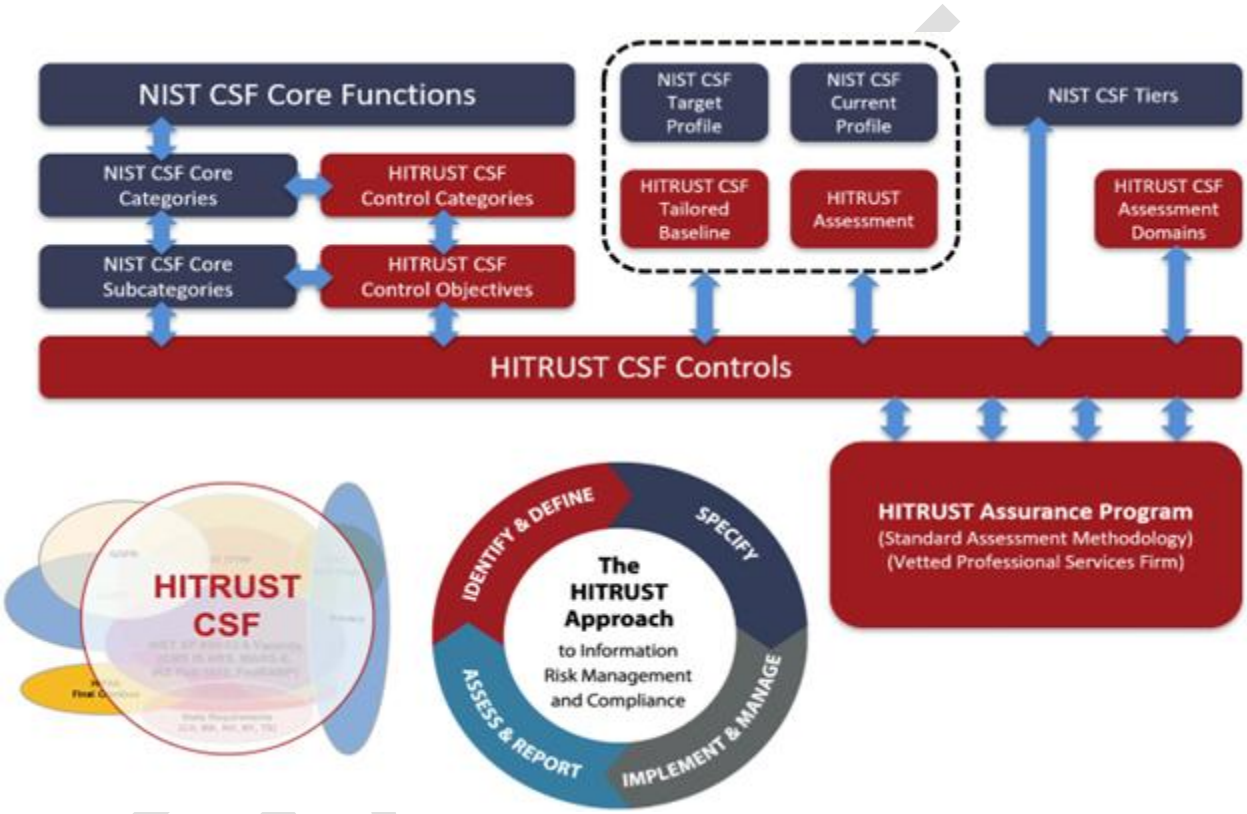

Figure 1. Implementing the NIST Cybersecurity Framework through the HITRUST CSF and CSF Assurance Program

The NIST CSF v2.0 Core is essentially a set of cybersecurity activities, desired outcomes, and applicable references that are common across government and industry. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across an organization from the executive level to the implementation/operations level, from one organization to another, and from one industry to another.

The Ransomware Community Profile

The Ransomware Community Profile discussed in NIST IR 8374 revision 1 is an overlay of the NIST CSF developed by NIST in collaboration with industry to serve as a baseline of NIST CSF

outcomes that address shared interests and goals among multiple organizations. It aligns organizations' ransomware prevention and mitigation requirements, objectives, risk appetite, and resources with elements of the NIST CSF.

The Ransomware Community Profile identifies a subset of NIST CSF categories and subcategories that are particularly relevant to mitigating ransomware risk.

Appendix A: Ransomware-relevant Observations

During the Essentials, 1-year (e1) validated assessment, no deficiencies were noted during the evaluation of any HITRUST CSF requirements mapping to the considered Ransomware requirements.

None identified

HITRUST

Appendix B: Relevant Assessment Results and Mappings

Below are the assessment results and control maturity evaluations for each assessed HITRUST CSF requirement mapped to the NIST Cybersecurity Framework V2.0.

In addition to relevant assessment results and control maturity evaluations, the table below lists the HITRUST CSF requirements mapped by HITRUST to each NIST Cybersecurity Framework (CSF) 2.0 subcategory. Note that many more mappings exist between the NIST CSF 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 Assessment Context section of this report.

The HITRUST CSF is mapped to dozens of other authoritative sources in addition to the NIST CSF, 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.

Govern

HITRUST CSF Requirements	Implemented Scoring
Organizational Context (GV.OC): The circumstances mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements surrounding the organizations cybersecurity risk management decisions are understood.	
GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	
BUID: 0101.00a1Organizational.123 / CVID: 0001.0. The organization has a formal information security management program (ISMP) that is documented and addresses the overall security program of the organization. Management support for the ISMP is demonstrated through signed acceptance or approval by management. The ISMP is based on	FC: Fully Compliant (100%)

HITRUST

HITRUST CSF Requirements	Implemented Scoring
an accepted industry framework, considers all the control objectives of the accepted industry framework, documents any excluded control objectives of the accepted industry framework and the reasons for their exclusion, and is updated at least annually or when there are significant changes in the environment.	
BUID: 01116.05bNYDOHOrganizational.6 / CVID: 2089.0. The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	FC: Fully Compliant (100%)
BUID: 0113.04a1Organizational.2 / CVID: 0431.1. The organization's information security policy is developed, published, disseminated, and implemented. The information security policy documents: state the purpose and scope of the policy; communicate management's commitment; describe management and workforce members' roles and responsibilities; and establish the organization's approach to managing information security.	FC: Fully Compliant (100%)
BUID: 0113.04a2Organizational.1 / CVID: 0431.2. As applicable to the focus of a security policy particular document, security policies contain: the organization's mission, vision, values, objectives, activities, and purpose, including the organization's place in critical infrastructure; a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing; a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives; a framework for setting control objectives and controls, including the structure of risk assessment and risk management; the need for information security; the goals of information security; the organization's compliance scope; legislative, regulatory, and contractual requirements, including those for the protection of covered information and the legal and ethical responsibilities to protect this information; arrangements for notification of information security incidents, including a channel for raising concerns regarding confidentially, without fear of blame or recrimination; a definition of general and specific responsibilities for information security management, including reporting information security incidents; references	FC: Fully Compliant (100%)

HITRUST CSF Requirements	Implemented Scoring
to documentation which may support the policy (e.g., more detailed security policies and procedures for specific information systems or security rules users comply with); a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization (including but not limited to CSF control objectives such as: (a) compliance with legislative, regulatory, and contractual requirements; (b) security education, training, and awareness requirements for the workforce, including researchers and research participants; (c) incident response and business continuity management; (d) consequences of information security policy violations; (e) continuous monitoring; (f) designating and maintaining an appropriately resourced and technically experienced information security team; (g) physical security of areas where sensitive information (e.g., PII, PCI and PMI data); and (h) coordination among organizational entities. As applicable to the focus of a security policy particular document, security policies also prescribe the development, dissemination, and review/update of formal, documented procedures to facilitate the implementation of security policy and associated security controls.	

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.