HITRUST

Ransomware Insights

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

Chinstrap Penguin Corporation

As of June 30, 2026

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

HITRUST

Contents

1. Transmittal Letter 3
2. Ransomware Scorecard 6
   Govern 7
3. Assessment Context 10
   About the HITRUST r2 Assessment and Certification 10
   Assessment Approach 10
   Risk Factors 11
4. Scope of the Assessment 14
5. Use of the Work of Others 17
6. Limitations of Assurance 18
7. Ransomware Overview 19
8. The NIST CSF and Ransomware Community Profile 20

Appendix A: Relevant Observations 21

Appendix B: Relevant Assessment Results and Mappings 22
   Govern 22

Appendix C: HITRUST Background 28

1. Transmittal Letter

June 30, 2026

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 Ransomware 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 HITRUST Risk-based, 2-year (r2) validated assessment using v11.4.0 of the HITRUST CSF. 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.

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.

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

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.

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

External Assessor Responsibilities

External Assessors are authorized by HITRUST based upon a thorough vetting process to demonstrate their ability to perform HITRUST CSF Assessments, and individual practitioners are required to maintain appropriate credentials based on their role in HITRUST assessments. In HITRUST validated assessments, the External Assessor is responsible for the following:

- Reviewing and gaining a detailed understanding of the information provided by the Organization.

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

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

HITRUST's Responsibilities

HITRUST is responsible for 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.

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

2. 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 Risk-based, 2-year (r2) validated assessment using v11.4.0 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). The Organization's scores are shown alongside the average control maturity scores across all r2 validated assessments submitted to HITRUST (labeled as "Avg. HITRUST r2 score"). Note that the Organization chose to exclude the measured and managed maturity levels from consideration in this assessment, making 75.00 (instead of 100.00) the highest maturity score directly achievable.

Scorecard Color Legend

Requirements met (Avg. score of mapped HITRUST CSF requirements: 70-79.9)
Requirements partially met (Avg. score of mapped HITRUST CSF requirements: 60-69.9)
Requirements not met (Avg. score of mapped HITRUST CSF requirements: <60)

HITRUST

Govern

GOVERN (GV): *The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored*

NIST CSF Core item	Priority	Ransomware Application	Average score in this assessment	Gaps noted in this asmt.
Organizational Context (GV.OC): The circumstances, mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements surrounding the organization's cybersecurity risk management decisions are understood				
GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	2	Priorities for organizational mission, objectives, and activities are established and communicated. Understanding priorities for organizational objectives and activities is needed to support contingency planning for future ransomware events and emergency response and recovery actions. For example, the most critical enterprise information and operational activities or functions might be given the highest priority for backup as well as for access management	75.00 / 75.00 Avg. HITRUST r2 score: 77.48	0
GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	1	Understanding the needs and expectations of internal and external stakeholders with respect to cybersecurity risk management is needed to support contingency planning for future ransomware events and emergency response and recovery actions (e.g., notification requirements). The priority for this outcome is designated Priority 1 because of both the importance of everyone understanding the consequences of a successful ransomware attack, and the need to understand the impact of the attack on specific internal and external stakeholders.	75.00 / 75.00 Avg. HITRUST r2 score: 77.43	0
GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity--including privacy and civil	2	Understanding legal and regulatory requirements regarding cybersecurity and privacy is necessary for organizational cybersecurity policy development and for establishing priorities in contingency planning for	75.00 / 75.00 Avg. HITRUST r2 score: 75.61	0

NIST CSF Core item	Priority	Ransomware Application	Average score in this assessment	Gaps noted in this asmt.
liberties obligations--are understood and managed		responses to and recovery from future ransomware events.		
Risk Management Strategy (GV.RM): The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions				
GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes	2	Ransomware risks must be factored into organizational risk management governance to support establishment of adequate organizational cybersecurity policies.	75.00 / 75.00 Avg. HITRUST r2 score: 74.63	0
Roles, Responsibilities, and Authorities (GV.RR): Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated				
GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced	1	Because ransomware events often result in the immediate loss of business functionality, organizations face extreme pressure to recover business functions quickly. Effective ransomware mitigation and response requires everyone in the organization understand their role, responsibility, and authority prior to a ransomware event. Because this is critical to mitigating ransomware impact and restoring business function, this outcome is designated Priority 1.	75.00 / 75.00 Avg. HITRUST r2 score: 72.89	0
Cybersecurity Supply Chain Risk Management (GV.SC): Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders				

NIST CSF Core item	Priority	Ransomware Application	Average score in this assessment	Gaps noted in this asmt.
GV.SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	1	Many ransomware events are enabled by some member of the workforce or a third-party stakeholder taking an intentional or inadvertent action that enables infiltration by criminals or other unauthorized parties. It's important to understand roles and responsibilities for preventing ransomware infections and the associated responsibilities with response and recovery actions. For this reason, the outcome is designated Priority 1.	75.00 / 75.00 Avg. HITRUST r2 score: 75.75	0
GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	2	Ransomware contingency planning should be coordinated with suppliers and third-party providers, and planning should include provision for testing of planned activities.	68.75 / 75.00 Avg. HITRUST r2 score: 75.73	1

Scorecard truncated in this example 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
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
Does the scoped environment allow dial-up/dial-in capabilities (i.e., functional analog modems)?	No
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
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
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
Is the scoped system(s) (on-premises or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)?	No
Does the system(s) transmit or receive data with a third-party?	No
Are hardware tokens used as an authentication method within the scoped environment?	No
Do any of the organization's personnel travel to locations the organization deems to be of significant risk?	No

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

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

HITRUST

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)

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 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 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 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.

7. 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.

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.

8. 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.

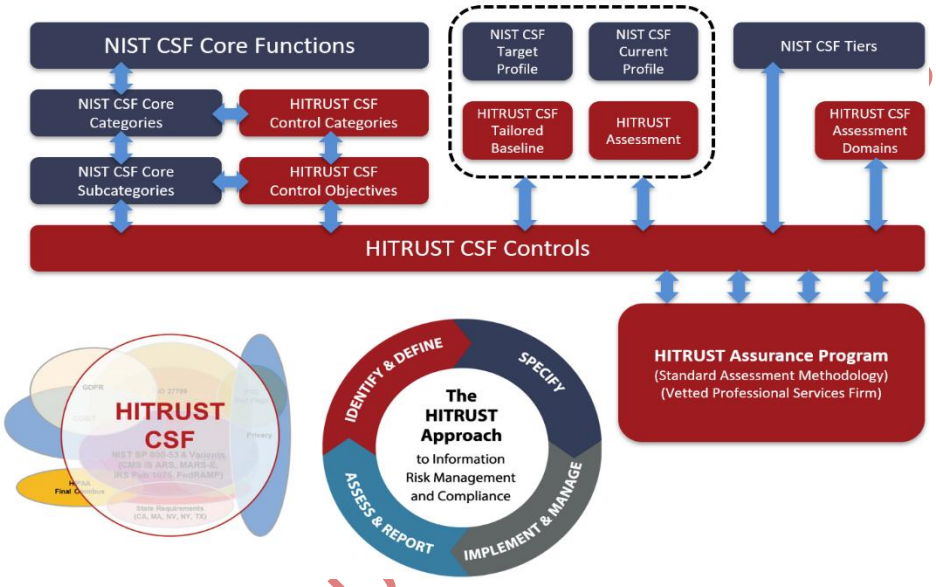

Figure 1. Implementing the NIST Cybersecurity Framework through the HITRUST CSF and CSF Assurance Program

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.

HITRUST

Appendix A: Relevant Observations

During the HITRUST r2 assessment underlying this report, the policy, procedure, and/or implemented control maturity level(s) on each of the following HITRUST CSF requirements scored less than "Fully Compliant". These conditions were identified as relevant to the Organization's ability to counter ransomware threats and/or to deal with the potential consequences of ransomware events, as each of these HITRUST CSF requirements map to one or more NIST CSF v2.0 subcategories including in the NIST CSF-based Ransomware Community Profile outlined in NIST IR 8374 revision 1. Those relying on this report should evaluate these items (and the associated risk treatment) in consultation with the Organization.

NIST CSF subcategory	Mapped HITRUST CSF requirement	Maturity level(s) scoring less than fully compliant	Corrective Action(s) [Unvalidated]
PR.AA-06	**Mapped BUID: 0321.09u1Organizational.2 / CVID: 1075.0** . The organization protects physical media housing covered and/or confidential information from unauthorized disclosure or modification while in transit by the appropriate application of at least one of the following: use of locked containers; delivery by hand; tamper-evident packaging (which reveals any attempt to gain access); or splitting of the consignment into more than one delivery and dispatch by different routes.	Implemented	*[Status: Not Started, Target Date: 3/31/2026]* Our asset inventory system shall include documentation to show that tamper evident packaging was utilized for all restricted removable media that is transported out of our facilities.
PR.PS-01, PR.PS-04	**Mapped BUID: 0629.10h2System.45 / CVID: 1308.0** . A rollback strategy is in place before changes are implemented. An audit log is maintained of all updates to operational program libraries.	Implemented	No corrective action plans were communicated to HITRUST for this condition.
PR.PS-06	**Mapped BUID: 06900.09d1System.2 / CVID: 1955.0** . The organization ensures separation between production and non-production (development, test/quality assurance) environments is established and controls are implemented to prevent operational issues.	Implemented	No corrective action plans were communicated to HITRUST for this condition.

Appendix A has been truncated for this sample report

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 subset of NIST Cybersecurity Framework core functions, categories, and subcategories prioritized in the Ransomware Community Profile as being particularly relevant to mitigating ransomware risk.

In addition to relevant assessment results and control maturity evaluations, the table below lists the HITRUST CSF requirements mapped by HITRUST to each identified NIST Cybersecurity Framework (CSF) v2.0 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 levels 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 Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
Organizational Context (GV.OC): The circumstances, mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements surrounding the organization's 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 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.	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)

HITRUST

HITRUST CSF Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
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%)	FC: Fully Compliant (100%)	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 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.	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)

HITRUST CSF Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
BUID: 0114.04b1Organizational.1 / CVID: 0435.0 . The information security policy documents are reviewed at planned intervals or if significant changes occur to ensure the policies' continuing adequacy and effectiveness. Security policies are communicated throughout the organization.	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)
BUID: 1701.03a1Organizational.12345678 / CVID: 0383.0 . The organization's risk management program includes: objectives of the risk management process; management's clearly stated level of acceptable risk, informed by its role in the critical infrastructure and business-specific risk analysis; the plan for managing operational risk communicated to stakeholders; the connection between the risk management policy and the organization's strategic planning processes; documented risk assessment processes and procedures; regular performance of risk assessments; mitigation of risks identified from risk assessments and threat monitoring procedures; risk tolerance thresholds are defined for each category of risk; reassessment of the risk management policy to ensure management's stated level of acceptable risk is still accurate, previously decided upon security controls are still applicable and effective, and to evaluate the possible risk level changes in the environment; updating the risk management policy if any of these elements have changed; and repeating the risk management process prior to any significant change, after a serious incident, whenever a new significant risk factor is identified, or at a minimum annually.	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)
GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered			

HITRUST

HITRUST CSF Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
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 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.	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)

HITRUST

HITRUST CSF Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
BUID: 1701.03a1Organizational.12345678 / CVID: 0383.0 . The organization's risk management program includes: objectives of the risk management process; management's clearly stated level of acceptable risk, informed by its role in the critical infrastructure and business-specific risk analysis; the plan for managing operational risk communicated to stakeholders; the connection between the risk management policy and the organization's strategic planning processes; documented risk assessment processes and procedures; regular performance of risk assessments; mitigation of risks identified from risk assessments and threat monitoring procedures; risk tolerance thresholds are defined for each category of risk; reassessment of the risk management policy to ensure management's stated level of acceptable risk is still accurate, previously decided upon security controls are still applicable and effective, and to evaluate the possible risk level changes in the environment; updating the risk management policy if any of these elements have changed; and repeating the risk management process prior to any significant change, after a serious incident, whenever a new significant risk factor is identified, or at a minimum annually.	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)
GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity--including privacy and civil liberties obligations--are understood and managed			
BUID: 0181.06a1Organizational.12 / CVID: 0543.0 . All relevant statutory, regulatory, and contractual requirements, including the specific controls and individual responsibilities to meet these requirements, are explicitly defined and formally documented (e.g., in policies and procedures, as appropriate) for each information system type, and communicated to the user community as necessary through documented security training and awareness programs.	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)
BUID: 1212.09ab2System.5 / CVID: 1147.0 . The organization complies with all relevant legal requirements applicable to its monitoring of authorized access and unauthorized access attempts.	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)

HITRUST CSF Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
BUID: 1701.03a1Organizational.12345678 / CVID: 0383.0 . The organization's risk management program includes: objectives of the risk management process; management's clearly stated level of acceptable risk, informed by its role in the critical infrastructure and business-specific risk analysis; the plan for managing operational risk communicated to stakeholders; the connection between the risk management policy and the organization's strategic planning processes; documented risk assessment processes and procedures; regular performance of risk assessments; mitigation of risks identified from risk assessments and threat monitoring procedures; risk tolerance thresholds are defined for each category of risk; reassessment of the risk management policy to ensure management's stated level of acceptable risk is still accurate, previously decided upon security controls are still applicable and effective, and to evaluate the possible risk level changes in the environment; updating the risk management policy if any of these elements have changed; and repeating the risk management process prior to any significant change, after a serious incident, whenever a new significant risk factor is identified, or at a minimum annually.	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)
BUID: 1857.08c1Organizational.1 / CVID: 0727.0 . Relevant health and safety regulations and standards are taken into consideration when securing facilities.	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)
BUID: 19131.05e1Organizational.45 / CVID: 0479.0 . Requirements for confidentiality and non-disclosure agreements are reviewed at least annually and when changes occur that influence these requirements. Confidentiality and non-disclosure agreements comply with all applicable laws and regulations for the jurisdiction to which it applies.	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)	FC: Fully Compliant (100%)

Appendix truncated in this example 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.