HITRUST

AI Risk Management Insights

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

Chinstrap Penguin Corporation

As of February 10, 2026

SAMPLE FOR ILLUSTRATIVE USE ONLY

HITRUST

Contents

HITRUST

1. Transmittal Letter

February 10, 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 Artificial Intelligence ("AI") Risk Management Insights Report at the request of Chinstrap Penguin Corporation ("the Organization"). This Insights Report contains detailed information regarding the Organization's AI risk management practices for the scope outlined below, based on a HITRUST Risk-based, 2-year (r2) Validated Assessment using v11.3.2 of the HITRUST CSF. This assessment included the HITRUST CSF requirements mapped to the following AI risk management authoritative sources: NIST AI Risk Management Framework v1.0 and ISO/IEC 23894:2023. The Organization can leverage this report to share information regarding their AI Risk Management 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 platform, facilities, and supporting infrastructure of the Organization ("Scope"):

Platform:

- Customer Central residing at Pelican Data Center

Facilities:

- CP Framingham Manufacturing Facility (Other) located in Framingham, Massachusetts, United States of America
- CP Headquarters and Manufacturing (Other) 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 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 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.

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

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 and an Authorized HITRUST External Assessor completed the accompanying Risk-based, 2-year (r2) validated. HITRUST is also responsible for producing the mappings from various authoritative sources, including NIST AI Risk Management Framework v1.0 and ISO/IEC 23894:2023, 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

2. AI Risk Management Scorecards

The tables below provide insights on AI risk management for the environment assessed, based on guidance contained in NIST AI Risk Management Framework v1.0 and ISO/IEC 23894:2023. Each requirement listed is assigned a compliance score for the policy, procedure, and implemented control maturity levels. These scores are based on the assessment results of the HITRUST CSF requirement(s) mapped to NIST AI Risk Management Framework v1.0 and ISO/IEC 23894:2023. These mappings can be found in Appendix B of this document.

The Organization may have in place additional controls relevant to their AI Risk Management program which were not evaluated in the underlying HITRUST assessment and therefore not reflected in this report.

To learn about the HITRUST control maturity evaluation and scoring approach, visit *https://hitrustalliance.net/content/uploads/Evaluating-Control-Maturity-Using-the-HITRUST-Approach.pdf.*

Scorecard Color Legend

FC	Fully Compliant: The control maturity level's scores across all HITRUST CSF requirements included in the Organization's HITRUST assessment mapped to the AI Risk Management requirement averaged 90 - 100%.
MC	Mostly Compliant: The control maturity level's scores across all HITRUST CSF requirements included in the Organization's HITRUST assessment mapped to the AI Risk Management requirement averaged 66 – 89.99%.

HITRUST

ISO/IEC 23894

Please refer to ISO/IEC 23894-available for purchase at *https://iso.org/*-for the content of each ISO/IEC 23894 requirement, as only identifiers and titles have been included in this Insights Report.

Part 5: Framework

Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
5.1. General				
5.1	General	FC	FC	FC
5.2. Leadership and commitment				
5.2	Leadership and commitment	FC	FC	FC
5.3. Integration				
5.3	Integration	FC	FC	FC
5.4. Design				
5.4.1	Understanding the organization and its context	FC	FC	FC
5.4.2	Articulating risk management commitment	FC	FC	FC
5.4.3	Assigning organizational roles, authorities, responsibilities and accountabilities	FC	FC	FC
5.4.4	Allocating resources	FC	FC	FC
5.4.5	Establishing communication and consultation	FC	FC	FC
5.5. Implementation				
5.5	Implementation	FC	FC	FC
5.6. Evaluation				
5.6	Evaluation	FC	FC	FC

Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
5.7. Improvement				
5.7.1	Adapting	FC	FC	FC
5.7.2	Continually improving	FC	FC	FC

Part 6: Process

Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
6.1. General				
6.1	General	FC	FC	MC
6.2. Communication and consultation				
6.2	Communication and consultation	FC	FC	FC
6.3. Scope, context and criteria				
6.3.1	General	FC	FC	FC
6.3.2	Defining the scope	FC	FC	FC
6.3.3	External and internal context	FC	FC	FC
6.3.4	Defining risk criteria	FC	FC	FC
6.4. Risk assessment				
6.4.1	General	FC	FC	FC
6.4.2.1	General	FC	FC	FC
6.4.2.2	Identification of assets and their value	FC	FC	FC
6.4.2.3	Identification of risk sources	FC	FC	FC
6.4.2.4	Identification of potential events and outcomes	FC	FC	FC
6.4.2.5	Identification of controls	FC	FC	FC
6.4.2.6	Identification of consequences	FC	FC	FC
6.4.3.1	General	FC	FC	FC
6.4.3.2	Assessment of consequences	FC	FC	FC

Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
6.4.3.3	Assessment of likelihood	FC	FC	FC
6.4.4	Risk evaluation	FC	FC	FC
6.5. Risk treatment				
6.5.1	General	Not Evaluated		
6.5.2	Selection of risk treatment options	FC	FC	FC
6.5.3	Preparing and implementing risk treatment plans	FC	FC	FC
6.6. Monitoring and review				
6.6	Monitoring and review	FC	FC	FC
6.7. Recording and reporting				
6.7	Recording and reporting	FC	FC	FC

NIST AI RMF

GOVERN

Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
GOVERN 1. Policies, processes, procedures, and practices across the organization related to the mapping, measuring, and managing of AI risks are in place, transparent, and implemented effectively				
GOVERN 1.1	Legal and regulatory requirements involving AI are understood, managed, and documented.	FC	FC	FC
GOVERN 1.2	The characteristics of trustworthy AI are integrated into organizational policies, processes, procedures, and practices.	FC	FC	FC

Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
GOVERN 1.3	Processes, procedures, and practices are in place to determine the needed level of risk management activities based on the organization's risk tolerance.	FC	FC	FC
GOVERN 1.4	The risk management process and its outcomes are established through transparent policies, procedures, and other controls based on organizational risk priorities.	FC	FC	FC
GOVERN 1.5	Ongoing monitoring and periodic review of the risk management process and its outcomes are planned and organizational roles and responsibilities clearly defined, including determining the frequency of periodic review.	FC	FC	FC
GOVERN 1.6	Mechanisms are in place to inventory AI systems and are resourced according to organizational risk priorities.	FC	FC	FC
GOVERN 1.7	Processes and procedures are in place for decommissioning and phasing out AI systems safely and in a manner that does not increase risks or decrease the organization's trustworthiness.	FC	FC	FC
GOVERN 2. Accountability structures are in place so that the appropriate teams and individuals are empowered, responsible, and trained for mapping, measuring, and managing AI risks.				
GOVERN 2.1	Roles and responsibilities and lines of communication related to mapping, measuring, and managing AI risks are documented and are clear to individuals and teams throughout the organization.	FC	FC	FC

Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
GOVERN 2.2	The organization's personnel and partners receive AI risk management training to enable them to perform their duties and responsibilities consistent with related policies, procedures, and agreements.	FC	FC	FC
GOVERN 2.3	Executive leadership of the organization takes responsibility for decisions about risks associated withAI system development and deployment.	FC	FC	FC
GOVERN 3. Workforce diversity, equity, inclusion, and accessibility processes are prioritized in the mapping, measuring, and managing of AI risks throughout the lifecycle.				
GOVERN 3.1	Decision-making related to mapping, measuring, and managing AI risks throughout the lifecycle is informed by a diverse team (e.g., diversity of demographics, disciplines, experience, expertise, and backgrounds).	FC	FC	FC
GOVERN 3.2	Policies and procedures are in place to define and differentiate roles and responsibilities for human-AI configurations and oversight of AI systems.	FC	FC	FC
GOVERN 4. Organizational teams are committed to a culture that considers and communicates AI risk.				
GOVERN 4.1	Organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of AI systems to minimize potential negative impacts.	FC	FC	FC

Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
GOVERN 4.2	Organizational teams document the risks and potential impacts of the AI technology they design, develop, deploy, evaluate, and use, and they communicate about the impacts more broadly.	FC	FC	FC
GOVERN 4.3	Organizational practices are in place to enable AI testing, identification of incidents, and information sharing.	FC	FC	FC
GOVERN 5. Processes are in place for robust engagement with relevant AI actors.				
GOVERN 5.1	Organizational policies and practices are in place to collect, consider, prioritize, and integrate feedback from those external to the team that developed or deployed the AI system regarding the potential individual and societal impacts related to AI risks.	FC	FC	FC
GOVERN 5.2	Mechanisms are established to enable the team that developed or deployed AI systems to regularly incorporate adjudicated feedback from relevant AI actors into system design and implementation.	FC	FC	FC
GOVERN 6. Policies and procedures are in place to address AI risks and benefits arising from third-party software and data and other supply chain issues.				
GOVERN 6.1	Policies and procedures are in place that address AI risks associated with third-party entities, including risks of infringement of a third-party's intellectual property or other rights.	FC	FC	FC
GOVERN 6.2	Contingency processes are in place to handle failures or incidents in third-party data or AI systems deemed to be high-risk.	FC	FC	FC

HITRUST

MANAGE

Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
MANAGE 1. AI risks based on assessments and other analytical output from the MAP and MEASURE functions are prioritized, responded to, and managed.				
MANAGE 1.1	A determination is made as to whether the AI system achieves its intended purposes and stated objectives and whether its development or deployment should proceed.	FC	FC	FC
MANAGE 1.2	Treatment of documented AI risks is prioritized based on impact, likelihood, and available resources or methods.	FC	FC	FC
MANAGE 1.3	Responses to the AI risks deemed high priority, as identified by the MAP function, are developed, planned, and documented. Risk response options can include mitigating, transferring, avoiding, or accepting.	FC	FC	FC
MANAGE 1.4	Negative residual risks (defined as the sum of all unmitigated risks) to both downstream acquirers of AI systems and end users are documented.	FC	FC	FC
MANAGE 2. Strategies to maximize AI benefits and minimize negative impacts are planned, prepared, implemented, documented, and informed by input from relevant AI actors.				
MANAGE 2.1	Resources required to manage AI risks are taken into account — along with viable non-AI alternative systems, approaches, or methods — to reduce the magnitude or likelihood of potential impacts.	FC	FC	FC
MANAGE 2.2	Mechanisms are in place and applied to sustain the value of deployed AI systems.	FC	FC	FC

Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
MANAGE 2.3	Procedures are followed to respond to and recover from a previously unknown risk when it is identified.	FC	FC	FC
MANAGE 2.4	Mechanisms are in place and applied, and responsibilities are assigned and understood, to supersede, disengage, or deactivate AI systems that demonstrate performance or outcomes inconsistent with intended use.	FC	FC	FC
MANAGE 3. AI risks and benefits from third-party entities are managed.				
MANAGE 3.1	AI risks and benefits from third-party resources are regularly monitored, and risk controls are applied and documented.	FC	FC	FC
MANAGE 3.2	Pre-trained models which are used for development are monitored as part of AI system regular monitoring and maintenance.	FC	FC	FC
MANAGE 4. Risk treatments, including response and recovery, and communication plans for the identified and measured AI risks are documented and monitored regularly.				
MANAGE 4.1	Post-deployment AI system monitoring plans are implemented, including mechanisms for capturing and evaluating input from users and other relevant AI actors, appeal and override, decommissioning, incident response, recovery, and change management.	FC	FC	FC
MANAGE 4.2	Measurable activities for continual improvements are integrated into AI system updates and include regular engagement with interested parties, including relevant AI actors.	FC	FC	FC

Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
MANAGE 4.3	Incidents and errors are communicated to relevant AI actors, including affected communities. Processes for tracking, responding to, and recovering from incidents and errors are followed and documented.	FC	FC	FC

MAP

Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
MAP 1. Context is established and understood.				
MAP 1.1	Intended purposes, potentially beneficial uses, context-specific laws, norms and expectations, and prospective settings in which the AI system will be deployed are understood and documented. Considerations include: the specific set or types of users along with their expectations; potential positive and negative impacts of system uses to individuals, communities, organizations, society, and the planet; assumptions and related limitations about AI system purposes, uses, and risks across the development or product AI lifecycle; and related TEVV and system metrics.	FC	FC	FC

Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
MAP 1.2	Interdisciplinary AI actors, competencies, skills, and capacities for establishing context reflect demographic diversity and broad domain and user experience expertise, and their participation is documented. Opportunities for interdisciplinary collaboration are prioritized.	FC	FC	FC
MAP 1.3	The organization's mission and relevant goals for AI technology are understood and documented.	FC	FC	FC
MAP 1.4	The business value or context of business use has been clearly defined or — in the case of assessing existing AI systems — re-evaluated.	FC	FC	FC
MAP 1.5	Organizational risk tolerances are determined and documented.	FC	FC	FC
MAP 1.6	System requirements (e.g., the system shall respect the privacy of its users) are elicited from and understood by relevant AI actors. Design decisions take socio-technical implications into account to address AI risks.	FC	FC	FC
MAP 2. Categorization of the AI system is performed.				
MAP 2.1	The specific tasks and methods used to implement the tasks that the AI system will support are defined (e.g., classifiers, generative models, recommenders).	FC	FC	FC

Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
MAP 2.2	Information about the AI system's knowledge limits and how system output may be utilized and overseen by humans is documented. Documentation provides sufficient information to assist relevant AI actors when making decisions and taking subsequent actions.	FC	FC	FC
MAP 2.3	Scientific integrity and TEVV considerations are identified and documented, including those related to experimental design, data collection and selection (e.g., availability, representativeness, suitability), system trustworthiness, and construct validation.	FC	FC	FC
MAP 3. AI capabilities, targeted usage, goals, and expected benefits and costs compared with appropriate benchmarks are understood.				
MAP 3.1	Potential benefits of intended AI system functionality and performance are examined and documented.	FC	FC	FC
MAP 3.2	Potential costs, including non-monetary costs, which result from expected or realized AI errors or system functionality and trustworthiness — as connected to organizational risk tolerance — are examined and documented.	FC	FC	FC
MAP 3.3	Targeted application scope is specified and documented based on the system's capability, established context, and AI system categorization.	FC	FC	FC

Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
MAP 3.4	Processes for operator and practitioner proficiency with AI system performance and trustworthiness — and relevant technical standards and certifications — are defined, assessed, and documented.	FC	FC	FC
MAP 3.5	Processes for human oversight are defined, assessed, and documented in accordance with organizational policies from the GOVERN function.	FC	FC	FC
MAP 4. Risks and benefits are mapped for all components of the AI system including third-party software and data.				
MAP 4.1	Approaches for mapping AI technology and legal risks of its components — including the use of third-party data or software — are in place, followed, and documented, as are risks of infringement of a third party's intellectual property or other rights.	FC	FC	FC
MAP 4.2	Internal risk controls for components of the AI system, including third-party AI technologies, are identified and documented.	FC	FC	FC
MAP 5. Impacts to individuals, groups, communities, organizations, and society are characterized.				
MAP 5.1	Likelihood and magnitude of each identified impact (both potentially beneficial and harmful) based on expected use, past uses of AI systems in similar contexts, public incident reports, feedback from those external to the team that developed or deployed the AI system, or other data are identified and documented.	FC	FC	FC

Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
MAP 5.2	Practices and personnel for supporting regular engagement with relevant AI actors and integrating feedback about positive, negative, and unanticipated impacts are in place and documented.	FC	FC	FC

MEASURE

Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
MEASURE 1. Appropriate methods and metrics are identified and applied.				
MEASURE 1.1	Approaches and metrics for measurement of AI risks enumerated during the MAP function are selected for implementation starting with the most significant AI risks. The risks or trustworthiness characteristics that will not — or cannot — be measured are properly documented.	FC	FC	FC
MEASURE 1.2	Appropriateness of AI metrics and effectiveness of existing controls are regularly assessed and updated, including reports of errors and potential impacts on affected communities.	FC	FC	FC

Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
MEASURE 1.3	Internal experts who did not serve as front-line developers for the system and/or independent assessors are involved in regular assessments and updates. Domain experts, users, AI actors external to the team that developed or deployed the AI system, and affected communities are consulted in support of assessments as necessary per organizational risk tolerance.	FC	FC	FC
MEASURE 2. Appropriate methods and metrics are identified and applied.				
MEASURE 2.1	Test sets, metrics, and details about the tools used during TEVV are documented.	FC	FC	FC
MEASURE 2.2	Evaluations involving human subjects meet applicable requirements (including human subject protection) and are representative of the relevant population.	FC	FC	FC
MEASURE 2.3	AI system performance or assurance criteria are measured qualitatively or quantitatively and demonstrated for conditions similar to deployment setting (s). Measures are documented.	FC	FC	FC
MEASURE 2.4	The functionality and behavior of the AI system and its components — as identified in the MAP function — are monitored when in production.	FC	FC	FC
MEASURE 2.5	The AI system to be deployed is demonstrated to be valid and reliable. Limitations of the generalizability beyond the conditions under which the technology was developed are documented.	FC	FC	FC

Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
MEASURE 2.6	The AI system is evaluated regularly for safety risks — as identified in the MAP function. The AI system to be deployed is demonstrated to be safe, its residual negative risk does not exceed the risk tolerance, and it can fail safely, particularly if made to operate beyond its knowledge limits. Safety metrics reflect system reliability and robustness, real-time monitoring, and response times for AI system failures.	FC	FC	FC
MEASURE 2.7	AI system security and resilience — as identified in the MAP function — are evaluated and documented.	FC	FC	FC
MEASURE 2.8	Risks associated with transparency and accountability — as identified in the MAP function — are examined and documented.	FC	FC	FC
MEASURE 2.9	The AI model is explained, validated, and documented, and AI system output is interpreted within its context — as identified in the MAP function — to inform responsible use and governance.	FC	FC	FC
MEASURE 2.10	Privacy risk of the AI system — as identified in the MAP function — is examined and documented.	FC	FC	FC
MEASURE 2.11	Fairness and bias — as identified in the MAP function — are evaluated and results are documented.	FC	FC	FC

Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
MEASURE 2.12	Environmental impact and sustainability of AI model training and management activities — as identified in the MAP function — are assessed and documented.	FC	FC	FC
MEASURE 2.13	Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented.	FC	FC	FC
MEASURE 3. Mechanisms for tracking identified AI risks over time are in place.				
MEASURE 3.1	Approaches, personnel, and documentation are in place to regularly identify and track existing, unanticipated, and emergent AI risks based on factors such as intended and actual performance in deployed contexts.	FC	FC	FC
MEASURE 3.2	Risk tracking approaches are considered for settings where AI risks are difficult to assess using currently available measurement techniques or where metrics are not yet available.	FC	FC	FC
MEASURE 3.3	Feedback processes for end users and impacted communities to report problems and appeal system outcomes are established and integrated into AI system evaluation metrics.	FC	FC	FC
MEASURE 4. Feedback about efficacy of measurement is gathered and assessed.				
MEASURE 4.1	Measurement approaches for identifying AI risks are connected to deployment context (s) and informed through consultation with domain experts and other end users. Approaches are documented.	FC	FC	FC

Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
MEASURE 4.2	Measurement results regarding AI system trustworthiness in deployment context (s) and across the AI lifecycle are informed by input from domain experts and relevant AI actors to validate whether the system is performing consistently as intended. Results are documented.	FC	FC	FC
MEASURE 4.3	Measurable performance improvements or declines based on consultations with relevant AI actors, including affected communities, and field data about context-relevant risks and trustworthiness characteristics are identified and documented.	FC	FC	FC

HITRUST

3. 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 into one of the largest specialty widget producers in the world. In 2014 the company entered the gadget market by acquiring Gadget Group and is now the third largest manufacturer of penguin gadgets in the US.

In-scope Platform

The following table describes the platform that was included in the scope of this assessment.

Customer Central (a.k.a. "Portal")	
Description	The Portal is a platform that allows numerous applications and service offerings to be accessed by customers via a single web-based interface via a browser. It does this for numerous customers and allows their customers to obtain information in a single location. Chinstrap Penguin personnel access the Portal through a secure VPN to a bastion host. From the bastion host systems administrators connect via VDI to an administrative console for management of all in-scope applications and supporting infrastructure. The Portal is developed by Chinstrap Penguin personnel. It is built in Java and .Net. The solution leverages VMWare for scalability. The applications/service offerings that make up the Portal are Penguin Nest, Penguin Analytics, and South Pole Benefit Eligibility. • Penguin Nest is an application that delivers content and applications from customer systems via the Portal. The application collects and feeds critical metrics to Penguin Analytics. • Penguin Analytics is an application that delivers reporting and analytics capability to customers. It allows them to develop dashboards and reports and track KPIs with their information that is stored within the Portal. • South Pole Benefits Eligibility allows our customers to provide benefit eligibility information so that users of the system have a single place to go to get the eligibility information from multiple customers. Meta data from the application is fed to Penguin Analytics for further analysis by customers.
Application(s)	Penguin Nest, Penguin Analytics, South Pole Benefits Eligibility
Database Type(s)	Oracle

Customer Central (a.k.a. "Portal")	
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

4. Use of the Work of Others

An *Authorized HITRUST External Assessor Organization* (i.e., the external assessor) performed procedures to validate the assessed entity'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 assessed entity (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

5. 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 AI risk management efforts 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 its AI risk management efforts and is not a certification of the NIST AI Risk Management Framework v1.0 or ISO/IEC 23894:2023.

- 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 AI risk management practices across the entirety of the Organization. Parties relying on this report should therefore evaluate the Scope in relation to the Organization's AI Risk Management obligations in consultation with the Organization.

    - Deficiencies noted in this report, if any, were identified through an evaluation of control maturity of the HITRUST CSF requirements mapping to NIST AI Risk Management Framework v1.0 and ISO/IEC 23894:2023 included in the Organization's HITRUST CSF Validated Assessment and not in observance of any other criteria specific to NIST AI Risk Management Framework v1.0 and ISO/IEC 23894:2023 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 conformity provides total assurance or 100% protection against possible control failures and instances of non-conformity. Because of their nature, controls may not prevent, or detect and correct, all errors or omissions relevant to compliance with standards or guidelines.

HITRUST

6. AI Risk Management Overview

Artificial Intelligence Risk Management encompasses a broad range of activities aimed at managing the risks that come with implementing and using AI technologies in an organization. It plays a crucial role in safeguarding against issues that might impact privacy, security, or financial stability, and ensures the responsible and secure adoption of AI.

Various frameworks have been developed to support AI Risk Management efforts, offering structured approaches for evaluating the ethical, legal, and technical aspects of AI systems. These frameworks often include guidelines for transparency, accountability, fairness, and safety, aiming to ensure AI systems are developed and used responsibly. Organizations might adopt international standards, industry-specific guidelines, or develop customized frameworks that align with their specific needs and the regulatory environment.

HITRUST strategically selected the NIST AI Risk Management Framework v1.0 and ISO/IEC 23894:2023 to assess AI Risk Management efforts, leveraging their complementary strengths. The NIST framework's flexibility complemented by ISO's directives ensures a robust evaluation of AI practices and effectively addresses both broad and specific risk considerations.

7. Coverage and Reportability

For specific HITRUST CSF control requirements mapping to NIST AI Risk Management Framework v1.0 and ISO/IEC 23894:2023, the Organization's HITRUST Validated Assessment provided information about how well they had been implemented and the nature and volume of identified gaps in implementation (if any). The HITRUST CSF and the inherent mappings to NIST AI Risk Management Framework v1.0 and ISO/IEC 23894:2023 as supported authoritative sources are important tools for organizations leveraging AI technologies.

The following factors collectively determined the degree of NIST AI Risk Management Framework v1.0 and ISO/IEC 23894:2023 coverage and reportability in the Organization's HITRUST assessment:

- HITRUST's approach to incorporating NIST AI Risk Management Framework v1.0 and ISO/IEC 23894:2023 into the HITRUST CSF.

- The Organization's assessment preferences and tailoring.

Approach to incorporating ISO/IEC 23894:2023 into the HITRUST CSF

ISO/IEC 23894:2023 is divided into three main parts:

- Clause 4, Principles: This clause describes the underlying principles of risk management.

- Clause 5, Framework: The purpose of the risk management framework is to assist the organization in integrating risk management into significant activities and functions.

- Clause 6, Processes: Risk management processes involve the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context, and assessing, treating, monitoring, reviewing, recording, and reporting risk.

ISO/IEC 23894 was not designed as a stand-alone document; instead, it is intended to be used in connection with ISO 31000-Risk Management. ISO 31000 provides guidance for risk management, and ISO/IEC 23894 provides specific guidance related to AI risk management. Because of this, HITRUST's ISO/IEC 23894 mappings also contain mappings to and coverage for ISO 31000-Risk Management.

The HITRUST CSF's coverage of ISO 31000 and ISO/IEC 23894 includes all of clauses 5 and 6 of both documents. Clause 4 of both documents was intentionally excluded from mapping consideration given its purely explanatory role.

HITRUST

Approach to incorporating NIST AI RMF v1.0 into the HITRUST CSF

The NIST AI Risk Management Framework is divided into two parts:

- Part 1 discusses how organizations can frame the risks related to AI and describes the intended audience. Next, AI risks and trustworthiness are analyzed, outlining the characteristics of trustworthy AI systems, which include valid and reliable, safe, secure and resilient, accountable and transparent, explainable and interpretable, privacy enhanced, and fair with their harmful biases managed.

- Part 2 comprises the "Core" of the Framework. It describes four specific functions to help organizations address the risks of AI systems in practice. These functions—GOVERN, MAP, MEASURE, and MANAGE—are broken down further into categories and subcategories.

HITRUST's mappings provide coverage for all of Part 2's functions, categories, and subcategories. Part 1 was intentionally excluded from mapping consideration given its purely explanatory role.

Why use both AI risk management documents?

The HITRUST CSF leverages concepts and content present in both of these respected AI risk management documents instead of just one or the other for the following reasons:

- Through its collection of functions, categories, and subcategories spanning all aspects of AI risk management, NIST AI RMF provides a rich hierarchy of AI risk management outcomes that organizations of varied sizes and complexities can aim for through a variety of approaches. Where the NIST AI RMF excels in flexibility, the ISO/IEC 23894 excels in prescriptiveness in that it contains specific, actionable AI risk management guidance. The NIST framework's flexibility complemented by ISO's specificity helps ensure robust evaluation and reporting of AI risk management practices.

- NIST prepared a crosswalk between these two documents, and HITRUST leveraged this crosswalk when harmonizing the contents of both documents into the HITRUST CSF. Thanks to this crosswalk HITRUST was able to map the HITRUST CSF requirements designed to meet ISO/IEC 23894 requirements to the corresponding requirements within NIST AI RMF.

- NIST publications are heavily leveraged within the United States, and ISO/IEC standards are heavily leveraged in Europe and other counties. A unified assessment avenue and assurance mechanism can better satisfy the needs of a globally diverse stakeholder group.

Impact of assessment preferences and tailoring on AI risk management reportability

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 Validated Assessments or can optionally utilize one of many prior

HITRUST CSF versions. As HITRUST advances the framework, more and better reporting capabilities are unlocked. Not all versions allow for the HITRUST insights reporting against the NIST AI Risk Management Framework v1.0 or ISO/IEC 23894:2023; only assessments utilizing version v11.3.2 and later can create this AI Risk Management Insights Report.

HITRUST

Appendix A: Relevant Observations

During the HITRUST Validated Assessment accompanying this AI Risk Management Insights Report, the policy, procedure, and/or implemented control maturity level(s) on the following HITRUST CSF requirement scored less than "Fully Compliant". This condition was identified as relevant to the Organization's AI Risk Management efforts, as this HITRUST CSF requirement map to one or more NIST AI Risk Management Framework v1.0 and/or ISO/IEC 23894:2023 requirements. The relying party should evaluate this item (and the associated risk treatment) in consultation with the Organization.

Mapped HITRUST CSF Requirement	Maturity level(s) scoring less than fully compliant	Mappings to considered AI Risk Management documents	Management's stated corrective actions (unvalidated)
BUID: 01.03aISO23894Organizational.25 / CVID: 2790.0. The organization aligns the AI system project-level processes with the organization s objectives.	Implemented	NIST AI RMF: 6.1 ISO/IEC 23894: GOVERN 2.3, GOVERN 3.2, MEASURE 2.2, MEASURE 2.8	No corrective action plans were communicated to HITRUST for this condition.

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 NIST AI Risk Management Framework v1.0 and ISO/IEC 23894:2023 considered in the underlying HITRUST CSF assessment

This section also shows the HITRUST CSF requirements mapped by HITRUST to each considered NIST AI Risk Management Framework v1.0 and ISO/IEC 23894:2023 requirement. Note that many more mappings exist between AI RM 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 AI RM Coverage and Reportability section of this document.

In addition to NIST AI Risk Management Framework v1.0 and ISO/IEC 23894:2023, 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.

Please refer to ISO/IEC 23894-available for purchase at *https://iso.org/*-for the content of each ISO/IEC 23894 requirement, as only identifiers and titles have been included in this Insights Report.

Part 5: Framework

HITRUST CSF Requirement	Policy Score	Process Score	Implemented Score
5.1 - General			
5.1 - ...			
Mapped BUID: 17.03aISO31000Organizational.4 / CVID: 2786.0. The organization evaluates its existing risk management practices and processes, evaluates any gaps, and addresses those gaps within an organization-chosen risk management framework on an annual basis. The characteristics of the chosen risk management framework (e.g., industry-accepted, regulatory-required) and the way in which they work together are customized and implemented to meet the needs of the organization.	Fully Compliant	Fully Compliant	Fully Compliant
5.2 - Leadership and commitment			
5.2 - ...			
Mapped BUID: 17.03aISO31000Organizational.4 / CVID: 2786.0. The organization evaluates its existing risk management practices and processes, evaluates any gaps, and addresses those gaps within an organization-chosen risk management framework on an annual basis. The characteristics of the chosen risk management framework (e.g., industry-accepted, regulatory-required) and the way in which they work together are customized and implemented to meet the needs of the organization.	Fully Compliant	Fully Compliant	Fully Compliant
Mapped BUID: 17.03aISO31000Organizational.9 / CVID: 2818.0. The organization ensures allocation of appropriate resources for risk management, including considerations for: people, skills, experience, and competence; the organization's processes, methods, and tools to be used for managing risk; documented processes and procedures; information and knowledge management systems; professional development and training needs; and capabilities of, and constraints on, existing resources.	Fully Compliant	Fully Compliant	Fully Compliant
Mapped BUID: 17.03aISO23894Organizational.21 / CVID: 2789.0. The organization allocates specialized resources to manage AI risk.	Fully Compliant	Fully Compliant	Fully Compliant

HITRUST CSF Requirement	Policy Score	Process Score	Implemented Score
Mapped BUID: 17.03aISO23894Organizational.20 / CVID: 2788.0. The organization issues statements related to its commitment to AI risk management to increase confidence of their stakeholders on their use of AI.	Fully Compliant	Fully Compliant	Fully Compliant
Mapped BUID: 17.03aISO23894Organizational.23 / CVID: 2787.0. The organization develops, documents, and disseminates policies and statements related to AI risks and risk management to stakeholders.	Fully Compliant	Fully Compliant	Fully Compliant
Mapped 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.	Fully Compliant	Fully Compliant	Fully Compliant

(The remainder of this subsection is redacted in this example report)

Part 6: Process

HITRUST CSF Requirement	Policy Score	Process Score	Implemented Score
6.1 - General			
6.1 - ...			
Mapped BUID: 17.03aISO31000Organizational.6 / CVID: 2812.0. The organization considers human behavior and culture throughout the risk management process.	Fully Compliant	Fully Compliant	Fully Compliant

HITRUST CSF Requirement	Policy Score	Process Score	Implemented Score
Mapped BUID: 17.03cISO23894Organizational.3 / CVID: 2795.0. The organization, using a risk-based process, identifies, assesses, understands, and takes appropriate treatment measures to address the AI risks to which they are exposed.	Fully Compliant	Fully Compliant	Fully Compliant
Mapped BUID: 01.03aISO23894Organizational.25 / CVID: 2790.0. The organization aligns the AI system project-level processes with the organization's objectives.	Fully Compliant	Fully Compliant	Mostly Compliant
Mapped 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.	Fully Compliant	Fully Compliant	Fully Compliant
6.2 - Communication and consultation			
6.2 - ...			
Mapped BUID: 17.03aISO31000Organizational.14 / CVID: 2819.0. The organization establishes a process to communicate and consult with stakeholders in order to support the risk management framework. Communication and consultation methods and content reflect the expectations of stakeholders, are timely, ensure that relevant information is collected, collated, synthesized and shared, as appropriate, and result in improvements being made based on feedback.	Fully Compliant	Fully Compliant	Fully Compliant

HITRUST CSF Requirement	Policy Score	Process Score	Implemented Score
Mapped 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.	Fully Compliant	Fully Compliant	Fully Compliant

(The remainder of this subsection is redacted in this example report)

GOVERN

HITRUST CSF Requirement	Policy Score	Process Score	Implemented Score
GOVERN 1 - Policies, processes, procedures, and practices across the organization related to the mapping, measuring, and managing of AI risks are in place, transparent, and implemented effectively			
GOVERN 1.1 - AI systems may be subject to specific applicable legal and regulatory requirements. Some legal requirements can mandate (e.g., nondiscrimination, data privacy and security controls) documentation, disclosure, and increased AI system transparency. These requirements are complex and may not be applicable or differ across applications and contexts. For example, AI system testing processes for bias measurement, such as disparate impact, are not applied uniformly within the legal context. Disparate impact is broadly defined as a facially neutral policy or practice that disproportionately harms a group based on a protected trait. Notably, some modeling algorithms or debiasing techniques that rely on demographic information, could also come into tension with legal prohibitions on disparate treatment (i.e., intentional discrimination). Additionally, some intended users of AI systems may not have consistent or reliable access to fundamental internet technologies (a phenomenon widely described as the digital divide) or may experience difficulties interacting with AI systems due to disabilities or impairments. Such factors may mean different communities experience bias or other negative impacts when trying to access AI systems. Failure to address such design issues may pose legal risks, for example in employment related activities affecting persons with disabilities.			
Mapped BUID: 17.03aISO31000Organizational.7 / CVID: 2815.0. The organization documents its external and internal context in the design of the risk management plan.	Fully Compliant	Fully Compliant	Fully Compliant

HITRUST CSF Requirement	Policy Score	Process Score	Implemented Score
Mapped BUID: 01.03aISO23894Organizational.13 / CVID: 2810.0. In support of the risk management process, the organization maintains documentation of the following aspects of the internal context of organization's development and/or use of AI: the effect that an AI system can have on the organization's culture by shifting and introducing new responsibilities, roles and tasks; any additional international, regional, national and local standards and guidelines that are imposed by the use of AI systems; the additional risks to organizational knowledge related to transparency and explainability of AI systems; the use of AI systems can result in changes to the number of human resources needed to realize a certain capability, or in a variation of the type of resources needed, for instance, deskilling or loss of expertise where human decision-making is increasingly supported by AI systems; the specific knowledge in AI technologies and data science required to develop and use AI systems; the availability of AI tools, platforms and libraries which can enable the development of AI systems without there being a full understanding of the technology, its limitations and potential pitfalls; the potential for AI to raise issues and opportunities related to intellectual property for specific AI systems; how AI systems can be used to automate, optimize and enhance data handling; as consumers of data, additional quality and completeness constraints on data and information can be imposed by AI systems; internal stakeholder perceptions, needs, and expectations; how the use of AI systems can increase the complexity of interdependencies and interconnections; the consideration that the use of AI systems can increase the need for specialized training.	Fully Compliant	Fully Compliant	Fully Compliant

HITRUST CSF Requirement	Policy Score	Process Score	Implemented Score
Mapped BUID: 01.03aISO23894Organizational.12 / CVID: 2809.0. In support of the risk management process, the organization maintains documentation of the following aspects of the external context of organization's development and/or use of AI: relevant legal requirements, including those specifically relating to AI; guidelines on ethical use and design of AI and automated systems issued by government-related groups, regulators, standardization bodies, civil society, academia and industry associations; domain-specific guidelines and frameworks related to AI; technology trends and advancements in the various areas of AI; societal and political implications of the deployment of AI systems, including guidance from social sciences; external stakeholder perceptions, needs, and expectations; how the use of AI, especially AI systems using continuous learning, can affect the ability of the organization to meet contractual obligations and guarantees; contractual relationships during the design and production of AI systems and services; how the use of AI can increase the complexity of networks and dependencies; and how an AI system can replace an existing system and, in such a case, an assessment of the risk benefits and risk transfers of an AI system versus the existing system can be undertaken, considering safety, environmental, social, technical and financial issues associated with the implementation of the AI system.	Fully Compliant	Fully Compliant	Fully Compliant

(The remainder of this subsection is redacted in this example report)

HITRUST CSF Requirement	Policy Score	Process Score	Implemented Score
MANAGE 1 - AI risks based on assessments and other analytical output from the MAP and MEASURE functions are prioritized, responded to, and managed.			
MANAGE 1.1 - AI systems may not necessarily be the right solution for a given business task or problem. A standard risk management practice is to formally weigh an AI system's negative risks against its benefits, and to determine if the AI system is an appropriate solution. Tradeoffs among trustworthiness characteristics —such as deciding to deploy a system based on system performance vs system transparency—may require regular assessment throughout the AI lifecycle.			
Mapped BUID: 17.03aISO31000Organizational.11 / CVID: 2821.0. The organization reviews the suitability, adequacy, and effectiveness of the organization-selected risk management framework and the way the risk management process is integrated into the organization at least annually. The organization implements relevant improvements and resolves gaps identified through this review.	Fully Compliant	Fully Compliant	Fully Compliant
Mapped BUID: 17.00aFedRAMPOrganizational.8 / CVID: 2395.0. The organization develops, documents, and disseminates to organization-defined personnel or roles a risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, and procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls. The organization reviews and updates the current risk assessment policy at least annually, and risk assessment procedures at least annually or whenever a significant change occurs.	Fully Compliant	Fully Compliant	Fully Compliant

HITRUST CSF Requirement	Policy Score	Process Score	Implemented Score
Mapped 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.	Fully Compliant	Fully Compliant	Fully Compliant

(The remainder of this subsection is redacted in this example report)

HITRUST CSF Requirement	Policy Score	Process Score	Implemented Score
MAP 1 - Context is established and understood.			
MAP 1.1 - Highly accurate and optimized systems can cause harm. Relatedly, organizations should expect broadly deployed AI tools to be reused, repurposed, and potentially misused regardless of intentions. AI actors can work collaboratively, and with external parties such as community groups, to help delineate the bounds of acceptable deployment, consider preferable alternatives, and identify principles and strategies to manage likely risks. Context mapping is the first step in this effort, and may include examination of the following: * intended purpose and impact of system use. * concept of operations. * intended, prospective, and actual deployment setting. * requirements for system deployment and operation. * end user and operator expectations. * specific set or types of end users. * potential negative impacts to individuals, groups, communities, organizations, and society — or context-specific impacts such as legal requirements or impacts to the environment. * unanticipated, downstream, or other unknown contextual factors. * how AI system changes connect to impacts.			
Mapped BUID: 17.03aISO31000Organizational.5 / CVID: 2822.0. The organization defines the scope of its risk management activities.	Fully Compliant	Fully Compliant	Fully Compliant
Mapped BUID: 17.03aISO31000Organizational.7 / CVID: 2815.0. The organization documents its external and internal context in the design of the risk management plan.	Fully Compliant	Fully Compliant	Fully Compliant

HITRUST CSF Requirement	Policy Score	Process Score	Implemented Score
Mapped BUID: 01.03aISO23894Organizational.13 / CVID: 2810.0. In support of the risk management process, the organization maintains documentation of the following aspects of the internal context of organization's development and/or use of AI: the effect that an AI system can have on the organization's culture by shifting and introducing new responsibilities, roles and tasks; any additional international, regional, national and local standards and guidelines that are imposed by the use of AI systems; the additional risks to organizational knowledge related to transparency and explainability of AI systems; the use of AI systems can result in changes to the number of human resources needed to realize a certain capability, or in a variation of the type of resources needed, for instance, deskilling or loss of expertise where human decision-making is increasingly supported by AI systems; the specific knowledge in AI technologies and data science required to develop and use AI systems; the availability of AI tools, platforms and libraries which can enable the development of AI systems without there being a full understanding of the technology, its limitations and potential pitfalls; the potential for AI to raise issues and opportunities related to intellectual property for specific AI systems; how AI systems can be used to automate, optimize and enhance data handling; as consumers of data, additional quality and completeness constraints on data and information can be imposed by AI systems; internal stakeholder perceptions, needs, and expectations; how the use of AI systems can increase the complexity of interdependencies and interconnections; the consideration that the use of AI systems can increase the need for specialized training.	Fully Compliant	Fully Compliant	Fully Compliant

HITRUST CSF Requirement	Policy Score	Process Score	Implemented Score
Mapped BUID: 01.03aISO23894Organizational.12 / CVID: 2809.0. In support of the risk management process, the organization maintains documentation of the following aspects of the external context of organization's development and/or use of AI: relevant legal requirements, including those specifically relating to AI; guidelines on ethical use and design of AI and automated systems issued by government-related groups, regulators, standardization bodies, civil society, academia and industry associations; domain-specific guidelines and frameworks related to AI; technology trends and advancements in the various areas of AI; societal and political implications of the deployment of AI systems, including guidance from social sciences; external stakeholder perceptions, needs, and expectations; how the use of AI, especially AI systems using continuous learning, can affect the ability of the organization to meet contractual obligations and guarantees; contractual relationships during the design and production of AI systems and services; how the use of AI can increase the complexity of networks and dependencies; and how an AI system can replace an existing system and, in such a case, an assessment of the risk benefits and risk transfers of an AI system versus the existing system can be undertaken, considering safety, environmental, social, technical and financial issues associated with the implementation of the AI system.	Fully Compliant	Fully Compliant	Fully Compliant
Mapped BUID: 17.03aISO23894Organizational.19 / CVID: 2798.0. The organization defines the scope of its risk management activities taking into consideration the objectives and purpose of the AI systems developed or used by the organization.	Fully Compliant	Fully Compliant	Fully Compliant

(The remainder of this subsection is redacted in this example report)

HITRUST CSF Requirement	Policy Score	Process Score	Implemented Score
MEASURE 1 - Appropriate methods and metrics are identified and applied.			
MEASURE 1.1 - The development and utility of trustworthy AI systems depends on reliable measurements and evaluations of underlying technologies and their use. Compared with traditional software systems, AI technologies bring new failure modes, inherent dependence on training data and methods which directly tie to data quality and representativeness. Additionally, AI systems are inherently socio-technical in nature, meaning they are influenced by societal dynamics and human behavior. AI risks — and benefits — can emerge from the interplay of technical aspects combined with societal factors related to how a system is used, its interactions with other AI systems, who operates it, and the social context in which it is deployed. In other words, What should be measured depends on the purpose, audience, and needs of the evaluations. These two factors influence selection of approaches and metrics for measurement of AI risks enumerated during the Map function. The AI landscape is evolving and so are the methods and metrics for AI measurement. The evolution of metrics is key to maintaining efficacy of the measures.			
Mapped BUID: 01.03aISO31000Organizational.1 / CVID: 2826.0. The organization, as part of the risk management process, considers the following when specifying risk criteria: the nature and type of uncertainties that can affect outcomes and objectives (both tangible and intangible), how consequences (both positive and negative) and likelihood will be defined and measured, time-related factors, consistency in the use of measurements, how the level of risk is to be determined, how combinations and sequences of multiple risks will be taken into account, and the organization's capacity.	Fully Compliant	Fully Compliant	Fully Compliant
Mapped BUID: 17.03aISO31000Organizational.15 / CVID: 2814.0. The organization establishes and implements standards for reporting risk management processes and results to stakeholders that consider differing stakeholders, and their specific information needs and requirements, cost, frequency, and timeliness of reporting, method(s) of reporting, and relevance of information to organizational objectives and decision-making.	Fully Compliant	Fully Compliant	Fully Compliant

HITRUST CSF Requirement	Policy Score	Process Score	Implemented Score
Mapped BUID: 17.03bISO23894Organizational.15 / CVID: 2808.0. The organization uses internal and external information on the trustworthiness of the AI system to assess for previously undetected risks or previously assessed risks that are no longer acceptable. If such a risk is identified, the organization assesses the effect on previous risk management activities and feeds the results of this assessment back into the risk management process. The assessment documentation contains: a description and identification of the system that has been analyzed; the methodology applied; a description of the intended use of the AI system; the identity of the person(s) and organization that carried out the risk assessment; the terms of reference and date of the risk assessment; the release status of the risk assessment; if and to what degree objectives have been met.	Fully Compliant	Fully Compliant	Fully Compliant
Mapped BUID: 17.03aISO23894Organizational.12 / CVID: 2802.0. To support the risk management process, the organization maintains documentation of the following: steps to understand uncertainty in all parts of the AI system, including the utilized data, software, mathematical models, physical extension, and human-in-the-loop aspects of the system; awareness that AI is a fast-moving technology domain. Measurement methods should be consistently evaluated according to their effectiveness and appropriateness for the AI systems in use; a consistent approach to determine the risk level. The approach should reflect the potential impact of AI systems regarding different AI-related objectives; consideration of the organization's AI capacity, knowledge level, and ability to mitigate realized AI risks when deciding its AI risk appetite.	Fully Compliant	Fully Compliant	Fully Compliant
Mapped BUID: 17.03aISO31000Organizational.10 / CVID: 2813.0. The organization documents and reports information about the risk management process and its results as defined in the risk management plan. The creation, retention, and handling of such documented information takes into account the use, sensitivity, and external and internal context.	Fully Compliant	Fully Compliant	Fully Compliant
MEASURE 1.2 - Different AI tasks, such as neural networks or natural language processing, benefit from different evaluation techniques. Use-case and particular settings in which the AI system is used also affects appropriateness of the evaluation techniques. Changes in the operational settings, data drift, model drift are among factors that suggest regularly assessing and updating appropriateness of AI metrics and their effectiveness can enhance reliability of AI system measurements.			

HITRUST CSF Requirement	Policy Score	Process Score	Implemented Score
Mapped BUID: 01.03aISO31000Organizational.2 / CVID: 2827.0. The organization, as part of risk identification, documents its consideration of: tangible and intangible sources of risk; causes and events; threats and opportunities; vulnerabilities and capabilities; changes in the external and internal context; indicators of emerging risks; the nature and value of assets and resources; consequences and their impact on objectives; limitations of knowledge and reliability of information; time-related factors; biases, assumptions and beliefs of those involved.	Fully Compliant	Fully Compliant	Fully Compliant
Mapped BUID: 01.03aISO31000Organizational.1 / CVID: 2826.0. The organization, as part of the risk management process, considers the following when specifying risk criteria: the nature and type of uncertainties that can affect outcomes and objectives (both tangible and intangible), how consequences (both positive and negative) and likelihood will be defined and measured, time-related factors, consistency in the use of measurements, how the level of risk is to be determined, how combinations and sequences of multiple risks will be taken into account, and the organization's capacity.	Fully Compliant	Fully Compliant	Fully Compliant

(The remainder of this subsection is redacted in this example report)

Appendix C: HITRUST Background

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

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

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

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

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

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

To learn about how HITRUST supports AI Risk Management, visit *https://hitrustalliance.net/ai-hub/.* For more information about HITRUST, the HITRUST CSF and other HITRUST offerings and programs, visit *https://hitrustalliance.net.*