HITRUST

AI Risk Management Insights

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

Chinstrap Penguin Corp

As of October 1, 2026

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

HITRUST

Contents

Transmittal Letter

October 1, 2026

Chinstrap Penguin Corp
123 Main Street
Anytown, Texas 12345

Through HITRUST's "Assess Once, Report Many" capability made possible through the HITRUST CSF, HITRUST has prepared this Artificial Intelligence Risk Management ("AI Risk Management") Insights Report at the request of Chinstrap Penguin Corp ("the Organization"). This Insights Report contains detailed information regarding the Organization's compliance with HITRUST CSF requirements mapping to NIST AI Risk Management Framework v1.0 and ISO/IEC 23894:2023 for the scope outlined below, based on a HITRUST Essentials, 1-year (e1) assessment using v11.6.0 of the HITRUST CSF. The Organization can leverage this report to share information regarding their AI Risk Management efforts with internal and external stakeholders.

The full e1 validated assessment report contains detailed information relating to the maturity of information protection controls as defined by the tailoring factors selected by management of the Organization. It includes detailed assessment results, a benchmark report comparing the Organization's results to industry results, and details on corrective action plans (if applicable). Such detailed information can best be leveraged by relying parties who are familiar with and understand the services provided by the Organization. Those interested in obtaining a copy of the full report should contact the Organization directly.

Scope

The e1 assessment that this Insights Report is based upon included the following platform, facilities, and supporting infrastructure of the Organization ("Scope"):

Platform:

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

Facilities:

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

The Organization's Responsibilities and Assertions

Management of the Organization is responsible for the implementation, operation, and monitoring of the control environment for the Scope. Through execution of this responsibility, and completion of a HITRUST Essentials, 1-year (e1) validated assessment, the Organization asserted that management of the Organization:

- Is responsible for the implementation of information protection controls.
- Disclosed all design and operating deficiencies in their information protection controls which they are aware, including those for which they believe the cost of corrective action may exceed the benefits.
- Is not aware of any events or transactions that have occurred or are pending that would have an effect on the Essentials, 1-year (e1) validated assessment that was performed and used as a basis by HITRUST for issuing that report.
- Is not aware of communications from regulatory agencies concerning noncompliance with or deficiencies regarding the information protection controls that are included within the scope of the Essentials, 1-year (e1) validated assessment.

Management of the Organization is also solely responsible for ensuring the Organization's compliance with any legal and/or regulatory requirements, including 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 completed the accompanying Essentials, 1-year (e1) validated assessment. 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.

Distribution and Use Restriction

This report is provided exclusively for the internal business use of Example Org. Distribution, publication, or disclosure of this report outside of Example Org, in whole or in part, is prohibited. This document contains recipient-specific identifying information and may be monitored for unauthorized distribution.

HITRUST

HITRUST

AI Risk Management Scorecards

The tables below provide insights on AI Risk Management for the environment, 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 implemented control maturity level. The compliance scores are based on the assessment results of the HITRUST CSF requirement(s) as mapped to the NIST AI Risk Management Framework v1.0 or ISO/IEC 23894:2023 requirement. The measured and managed control maturity levels are not included in this scorecard, as these control maturity levels were not assessed in the underlying HITRUST CSF assessment as a result of the Organization's assessment tailoring. 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

PC	Partially 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 33 - 65.99%.
MC	Mostly Compliant: The control maturity level's scores across all HITRUST CSF requirements included in the Organization's HITRUST assessment mapped to the AI Risk Management requirement averaged 66 - 89.99%.
FC	Fully Compliant: The control maturity level's scores across all HITRUST CSF requirements included in the Organization's HITRUST assessment mapped to the AI Risk Management requirement averaged 90 - 100%.

HITRUST

NIST AI RMF v1.0 Scorecard

GOVERN

Reference	Requirement	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
GOVERN 1.2	The characteristics of trustworthy AI are integrated into organizational policies, processes, procedures, and practices.	FC
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
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
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
GOVERN 1.6	Mechanisms are in place to inventory AI systems and are resourced according to organizational risk priorities.	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
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

Reference	Requirement	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
GOVERN 2.3	Executive leadership of the organization takes responsibility for decisions about risks associated with AI system development and deployment.	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
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
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
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
GOVERN 4.3	Organizational practices are in place to enable AI testing, identification of incidents, and information sharing.	FC

This section has been truncated for this sample report

HITRUST

ISO/IEC 23894:2023 Scorecard

Please refer to ISO/IEC 23894:2023—available for purchase at https://iso.org/—for the content of each ISO/IEC 23894:2023 requirement, as only identifiers and titles have been included in this Insights Report.

Part 5: Framework

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

This section has been truncated for this sample report

HITRUST

Scope of the Assessment

Company Background

Chinstrap Penguin Corp is a manufacturer, retailer and distributor of widgets for use in the care, feeding and housing of all Antarctic Chinstrap Penguins. Chinstrap Penguin Corp was established in 2005 and has grown to one of the largest widget producers in the world and now offers a number of specialized widgets to its customers and third-party distributors. In 2014 Chinstrap Penguin Corp entered the gadget market by acquiring Gadget Group and is now the third largest gadget manufacturer in the United States.

In-Scope Platform

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

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

Customer Central (a.k.a. "Portal")	
Residing Facility	Pelican Data Center
Exclusion(s) from scope	None

In-Scope Facilities

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

Facility Name	Type of Facility	Third-party Managed?	Third-party Provider	City	State	Country
CP Framingham Manufacturing Facility	Office	No	-	Framingham	MA	United States of America
CP Headquarters and Manufacturing	Office	No	-	Las Vegas	NV	United States of America
Pelican Data Center	Data Center	Yes	Pelican Hosting	Salt Lake City	UT	United States of America

Services Outsourced

The following table presents outsourced services relevant to the scope of this assessment. The "Consideration in this Assessment" column of this table specifies the method utilized for each service provider relevant to the scope of this e1 assessment. Organizations undergoing e1 assessments have two options of how to address situations in which a HITRUST CSF requirement is fully or partially performed by a service provider (e.g., by a cloud service provider):

- The Inclusive method, whereby HITRUST CSF requirements performed by the service provider are included within the scope of the assessment and addressed through full or partial inheritance, reliance on third-party assurance reports, and/or direct testing by the external assessor, and

- The Exclusive (or Carve-out) method, whereby HITRUST CSF requirements performed by the service provider are excluded from the scope of the assessment and marked N/A with supporting commentary explaining that the HITRUST CSF requirement is fully performed by a party other than the assessed entity (for fully outsourced controls) or through commentary explaining the excluded partial performance of the HITRUST CSF requirement (for partially outsourced controls).

Third-party Provider	Relevant Service(s) Provided	Consideration in this Assessment
Pelican Hosting	Pelican Hosting provides a colocation facility where Chinstrap maintains a dedicated cage. Pelican Hosting personnel do not have logical access to any in-scope systems.	Included

HITRUST

Use of the Work of Others

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

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

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

Assessment Utilized	Assessed Entity	Assessment Type	Utilization Approach	Relevant Platforms	Relevant Facilities	Assessment Domains
Pelican Hosting HITRUST r2	Pelican Hosting	HITRUST r2	Inheritance	(All in-scope platforms)	(All in-scope facilities)	(All assessment domains)

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 NIST AI Risk Management Framework v1.0 or ISO/IEC 23894:2023 compliance.

- This Insights Report accompanies a HITRUST CSF e1 Validated assessment. The accompanying e1 Validated assessment was scoped and performed in accordance with the HITRUST Assurance Program requirements designed to measure and report on control maturity for purposes of issuing HITRUST validated assessment reports. Consequently:

    - HITRUST assessments are scoped based on a defined boundary inclusive of specified management systems, physical facilities and IT platforms. Therefore, the HITRUST assessment may be scoped differently than an assessment focused exclusively to evaluate AI Risk Management practices across the entirety of the Organization.

    - Compliance 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 validated assessment and not in observance of any other criteria specific to NIST AI Risk Management Framework v1.0 and ISO/IEC 23894:2023.

- 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

AI Risk Management Overview

AI 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 RMF 1.0 and ISO 23894 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.

Coverage and Reportability

For specific HITRUST CSF control requirements mapping to ISO/IEC 23894:2023 and NIST AI RMF v1.0, 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 ISO/IEC 23894:2023 and NIST AI RMF v1.0 as supported authoritative sources are important tools for organizations leveraging AI technologies.

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

- HITRUST's approach to incorporating ISO/IEC 23894:2023 and NIST AI RMF v1.0 into the HITRUST CSF
- The Organization's assessment preferences and tailoring

Approach to incorporating ISO/IEC 23894:2023 and NIST AI RMF v1.0 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 23894:2023 was not designed as a stand-alone document; instead, it is intended to be used in connection with ISO 31000:2018—Risk Management. ISO 31000:2018 provides guidance for risk management, and ISO/IEC 23894:2023 provides specific guidance related to AI risk management. Because of this, HITRUST's ISO/IEC 23894:2023 mappings also contain mappings to and coverage for ISO 31000:2018—Risk Management.

The HITRUST CSF's coverage of ISO 31000:2018 and ISO/IEC 23894:2023 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

NIST AI RMF v1.0 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 23894:2023 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 23894:2023 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.

HITRUST

Impact of assessment preferences and tailoring on AI risk management reportability

HITRUST assessments are performed against a subset of HITRUST CSF's numerous requirements. The requirements included in the accompanying HITRUST Essentials, 1-year (e1) assessment have been tailored based on the unique risks and compliance needs of the Organization and on the HITRUST CSF version selected by the Organization (v11.6.0).

Through tailoring, organizations can optionally add authoritative sources into their Essentials, 1-year (e1) assessments. When this occurs, the assessment is expanded to consider additional requirements mapping to the information security and/or privacy-related portions of the included authoritative sources. The resulting, tailored HITRUST Essentials, 1-year (e1) assessment then serves to directly evaluate the Organization's adherence to a subset of the HITRUST CSF and indirectly evaluate the assessed entity's compliance with the information security and/or privacy aspects of the included authoritative source(s).

The HITRUST CSF is constantly updated by HITRUST in response to changes in the cybersecurity threat landscape and updates to included authoritative sources. Organizations can utilize the most recent HITRUST CSF version in HITRUST Essentials, 1-year (e1) 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 NIST AI RMF v1.0 and ISO/IEC 23894:2023; instead, only assessments utilizing version v11.6.0 and later can create this AI Risk Management Insights Report.

HITRUST

Appendix A: AI Risk Management-relevant Observations

During the HITRUST assessment accompanying this AI Risk Management Insights Report, the implemented control maturity level on each of the following HITRUST CSF requirements scored less than "Fully Compliant". These conditions were identified as relevant to the Organization's AI Risk Management efforts, as each of these HITRUST CSF requirements map to one or more NIST AI Risk Management Framework v1.0 and/or ISO/IEC 23894:2023 requirements. The relying party should evaluate these items (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 mgt. documents	Management's stated corrective actions (unvalidated)
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.	Implemented	NIST AI RMF v1.0: MAP 1.5, MEASURE 2.2, GOVERN 4.3, MAP 2.3, MEASURE 4.1, MANAGE 4.2, MEASURE 1.1, MEASURE 2.13, MEASURE 1.2, MAP 5.1, MEASURE 2.5 ISO/IEC 23894:2023: 6.3.4, 6.4.3.3	No corrective action plans were communicated to HITRUST for this condition.

HITRUST

Appendix B: Relevant HITRUST Assessment Results and Mappings

Below are the assessment results and control maturity evaluations for each assessed HITRUST CSF requirement mapped to the areas of NIST AI Risk Management Framework v1.0 and ISO/IEC 23894:2023 considered in the underlying HITRUST CSF assessment, organized by NIST AI Risk Management Framework v1.0 and ISO/IEC 23894:2023 part.

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.

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.

NIST AI RMF v1.0

GOVERN

HITRUST CSF Requirement	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: Legal and regulatory requirements involving AI are understood, managed, and documented. 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	

HITRUST CSF Requirement	Implemented Score
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.	
BUID: 01.03aISO23894Organizational.12 / CVID: 2809.0. The organization maintains documentation of the following aspects of the external context of organizations 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
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

This section has been truncated for this sample report

HITRUST

ISO/IEC 23894:2023

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	Implemented Score
5.1: General	
5.1: General	
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
5.2: Leadership and commitment	
5.2: Leadership and commitment	
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

This section has been truncated for this sample report

HITRUST

Appendix C: HITRUST Background

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

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

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

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

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

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

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.